Unicenter

NetMaster Network Management for TCP/IP User Guide

Version 6.2

Computer Associates

The Software That Manages eBusiness

Booklist

Contents

Chapter 1: About NetMaster for TCP/IP

Features and Benefits of NetMaster for TCP/IP 1-2
- Management of TN3270 Sessions 1-3
- Monitoring and Control of FTP Connections 1-3
- Logging and Reporting of TCP/IP Activities 1-4
- Monitoring of Network Events and Responses 1-4
- Packet Tracing for TCP/IP Environments 1-4
- Monitoring of Critical IP Resources 1-5
- Web User Interface 1-6
- Transaction Path Analyzer 1-9
- 2216 Router and TN3270 Server Support 1-9
- Cisco Channel Card and TN3270 Server Support 1-10
- Visibility and Management of SNMP 1-11
- Integrated Management of Multiple Systems 1-11
- Real-time Performance Monitor 1-11
- Performance Monitoring 1-12
- Command and Resource-based Security 1-13
- Open Systems Adapters (OSA) 1-14
- Communications Storage Manager (CSM) 1-14
- Address Space 1-14
- Enterprise Extender 1-14

TCP/IP Stack Support 1-15
Network Scenarios and NetMaster for TCP/IP Features 1-15

Chapter 2: Getting Started

Accessing and Leaving the NetMaster for TCP/IP Region 2-2
Logging On 2-2
Logging Off 2-3
Changing Your Password 2-3
Authority Levels 2-5
Accessing Functions 2-5
Selecting an Option 2-5
Selecting a Function Directly—Using Shortcuts 2-6
Selecting a Function Directly—Skipping Panels 2-7
Using Lists 2-8
Scrolling 2-8
Searching for an Item in Retrieved Information 2-10
Using Data Entry Panels 2-10
Switching to UPDATE Mode 2-10
Entering Data 2-11
Validating and Filing Data 2-11
Moving Between Panels 2-11
Getting Help 2-13
Using the Tip of the Day 2-13
Getting Help About a Panel 2-14
Getting Help About a Message 2-14
Working in Two Windows 2-15
Splitting Screens 2-15
Swapping Screens 2-15

Chapter 3: Managing Connections

About Connection Lists 3-2
Types of Connection Lists 3-2
Connection List Criteria 3-3
Listing Connections for Multiple Systems 3-5
Sorting Connection Lists 3-6
Locating Information on Connection Lists 3-6
Listing Telnet Connections 3-7
Telnet Connection List Criteria 3-7
Telnet Connection List 3-8
Listing CICS Socket Connections 3-9
CICS Socket Connection List Criteria 3-9
CICS Socket Connection List 3-10

Listing General Connections 3-11
Connection List Criteria 3-12
Connection List 3-12
Displaying Connection Information 3-14
Displaying Connections Graphically 3-14
Displaying Telnet Connections 3-15
Displaying CICS Socket Connections 3-16
Displaying General Connections 3-17
Displaying Status of TCP/IP Resources 3-18
Listing Specific Connections 3-18
Finding an LU Name 3-18
Finding an IP Address 3-19

Chapter 4: Diagnosing Connection Problems

Testing Connectivity 4-2
Performing a Ping 4-2
Interpreting Responses to a Ping 4-3
Using the PING Line Command 4-4
Tracing a TCP/IP Route 4-4
Performing a Traceroute 4-4
Interpreting Responses to a Traceroute 4-5
Initiating a Traceroute by Using the TRACEROUTE Line Command 4-6
Checking for SNA Related Problems on Telnet Connections 4-7
Checking the VTAM Status of an LU 4-7
Analyzing SNA Sessions 4-8
Looking Up a Device Name 4-9
Initiating a Lookup Using the NSLOOKUP Line Command 4-9
Dropping a Connection 4-9
Diagnosing Data and Protocol Related Problems in a Connection 4-10
Browsing the Local or Remote Activity Logs 4-10
Customizing the Activity Log 4-11
Telnet Activity in the Log 4-11
FTP Activity in the Log 4-12
Connection Activity in the Log 4-13
Diagnosing Telnet Response Time Problems 4-13
Viewing End-to-end Response Times 4-13
Diagnosing Throughput of Data Transfers 4-15
Viewing End-to-end Throughput 4-16

Monitoring FTP Workload Performance 4-17
Monitoring Connection Workload Performance 4-18
Monitoring Telnet Workload Performance 4-19

Chapter 5: Managing IP Resources

Managing IP Resources 5-2
Monitoring IP Resources 5-2
Customizing Display Attributes and Formats 5-3
Filtering IP Resources 5-3
User Profile 5-3
Commands on the IP Resource Monitor 5-3
IP Resource Classes 5-4
Adding an IP Resource to the IP Resource Monitor 5-4

Chapter 6: Diagnosing the IBM TCP/IP Environment

Managing Your IBM IP Stack 6-2
IP Resource Commands 6-2
Displaying Device Links 6-4
Displaying Device Links Graphically 6-5
Monitoring Stack IP Performance 6-7
Monitoring Stack IP Performance History 6-7
Monitoring Stack IP Performance Metrics 6-8
Monitoring Interface Workload Performance 6-9
Issuing Console Commands 6-9
Browsing and Changing the IBM Configuration Datasets 6-10
Browsing and Changing the TCP/IP Configuration 6-10
Browsing and Changing the Client Configuration 6-12
Browsing and Changing the FTP Server Configuration 6-13
Browsing the TCP/IP Error Log 6-14
Changing the Configuration by Using an Obeyfile Dataset 6-15
Checking Your Obeyfile Results 6-16
Other Actions on the TCP/IP Obeyfile PDS List Panel 6-16
Editing an Obeyfile Dataset 6-16
Checking Telnet LUs 6-18
Displaying Workload of Multiple TCP/IP Stacks 6-19
Displaying the Workload of Telnet Servers 6-19

Chapter 7: Diagnosing the TCPaccess Environment

Managing Your TCPaccess IP Stack 7-2
IP Resource Commands 7-2
Displaying Device Links 7-4
Displaying Device Links Graphically 7-4
Monitoring Stack IP Performance 7-7
Monitoring Stack IP Performance History 7-7
Monitoring Stack IP Performance Metrics 7-8
Monitoring Interface Workload Performance 7-9
Issuing Console Commands 7-9
Browsing and Changing the Parameters Library 7-10
Browsing and Changing a PARMS Member 7-11

Chapter 8: Managing Open Systems Adapters

About Open Systems Adapters (OSA) 8-2
Managing OSAs 8-2
IP Resource Commands 8-3
Displaying OSA Utilization 8-4
Monitoring OSA Performance 8-4
Listing OSA Devices 8-5
Monitoring OSA and Device Performance 8-6
Displaying OSA Configuration 8-6

Chapter 9: Managing Cisco Channel Cards

About Cisco Channel Cards 9-2
Monitoring Channel Cards 9-3
Diagnosing Telnet Connection Problems 9-3
Viewing a Telnet LU Mini Trace 9-4
Managing Channel Cards 9-4
IP Resource Commands 9-5
Displaying Channel Card Information 9-7
Displaying Application Information 9-7
Starting a Telnet Connection to the Router 9-8
Displaying Channel Information 9-8
Displaying TN3270 Server Information 9-9
Function Keys on the Cisco TN3270 Server Information Panel 9-9
Listing PUs for a Server 9-10
Listing LUs for a PU 9-11

Displaying the TN3270 Server Log 9-12
Displaying CLAW Information 9-13
Displaying CLAW Subchannel Information 9-14
Sorting Entries on the Cisco CLAW Subchannel List 9-16
Displaying TCP Offload Information 9-17
Displaying CSNA Information 9-18
Displaying Internal LAN Information 9-19
Displaying Internal LAN Adapters 9-19
Monitoring Channel Card Performance 9-20

Chapter 10: Managing 2216 Routers

Managing 2216 Routers 10-2
IP Resource Commands 10-2
Displaying 2216 Router Information 10-4
Displaying TN3270 Server Information 10-5
Displaying TN3270 PU Information 10-5
Displaying TN3270 LU Information 10-6
Displaying Channel Information 10-6
ESCON Connection Hierarchy 10-6
Monitoring 2216 Router Performance 10-7

Chapter 11: Managing Enterprise Extender

About Enterprise Extender 11-2
Managing Enterprise Extender 11-2
IP Resource Commands 11-3
Displaying XCA Major Node Summary 11-4
Displaying XCA Major Node 11-4
Displaying Additional Information 11-5
Listing Sessions 11-5
Displaying UDP Port Activity 11-6
Monitoring Enterprise Extender Performance 11-7

Chapter 12: Monitoring CSM Resources

Monitoring Your CSM Resources 12-2
IP Resource Commands 12-2
Displaying CSM Usage 12-4
Monitoring CSM Performance 12-5

Chapter 13: Monitoring Address Spaces

Monitoring Your Address Spaces 13-2
IP Resource Commands 13-2
Monitoring Address Space Performance 13-3

Chapter 14: Monitoring CICS Resources

Monitoring Your CICS Resources 14-2
IP Resource Commands 14-3
Listing CICS Connections from a Socket Management Perspective 14-4
Displaying Information About a CICMON Resource 14-4
Shutting Down and Restarting Socket Management for CICS and CPT 14-5
Stopping and Restarting the Command Server Interface 14-6
Starting a CICS Server 14-7
Starting CICS Transactions 14-8
Monitoring CICS Resource Performance 14-9

Chapter 15: Monitoring Alerts and IP Nodes

Monitoring Active Alerts 15-2
Commands on the Alert Monitor Panel 15-3
Working with Alerts 15-4
Raising Trouble Tickets for Alerts 15-4
Displaying Alert Details 15-5
Printing Alert Details 15-6
Displaying Alert History 15-6
Commands on the Alert History Panel 15-6
Monitoring IP Nodes 15-7
Filtering IP Nodes 15-8
Adding an IP Node to Be Monitored 15-8

Chapter 16: Diagnosing Printer Problems

Determining Printer Problems 16-2
Querying Printer Status 16-2
Deleting an Entry in the Print Queue 16-3
Sending a Test Print 16-4

Chapter 17: Producing Reports

About Reports 17-2
Online Reporting 17-2
Listing and Viewing Reports 17-3
Actions on the History Report List 17-3
Searching the TCP/IP Events Database 17-4
Searching Connections 17-4
Searching File Transfer Events 17-5
Searching Telnet Connections 17-5
Performing a Custom Search 17-6
Examples of Custom Searches 17-7
Actions on the Search Criteria Panel 17-8
Searching Sampled Performance Data 17-9
Extracting Data to a File 17-10
Printing Reports 17-11
Checking the Print Queue 17-12
Defining Printed Reports 17-12
Long-range Reporting Using the Offline Archival System 17-13

Chapter 18: Reporting Real-time Performance

Monitoring Real-time Performance 18-2
Displaying Performance History 18-2
Listing Resource Attributes of Performance Samples 18-4
Diagnosing Resource Attributes 18-4
Information on the Bar Charts 18-5
Displaying the Resource Summary Graph 18-6
Displaying the Resource Detail Graph 18-6

Chapter 19: Diagnosing IP Networks

Network Diagnosis Functions Menu 19-2
Network Diagnosis Functions Menu Options 19-2
Input Fields on the Network Diagnosis Functions Menu 19-3
Browsing System Information 19-4
Browsing the Interface List 19-5
Displaying a Routing Table 19-6
Actions on the Routing Table 19-7
Viewing SNMP Functions 19-8

Chapter 20: Collecting and Using Trace Data

Tracing IP Packets in TCP/IP 20-2
Packet Tracing Menu 20-2
Packet Tracing Menu Options 20-3
Input Fields on the Packet Tracing Menu 20-3
Performing a Trace and Saving Data 20-4
Sequence of Actions 20-4
Starting CTRACE 20-5
Starting a Trace 20-6
Starting a Trace from the Packet Tracing Menu 20-6
Starting a Trace from a Connection List 20-7
Listing Active Traces 20-7
Stopping a Trace 20-7
Stopping a Trace from the Packet Tracing Menu 20-8
Stopping a Trace from a Connection List 20-8
Stopping CTRACE 20-9
Saving the CTRACE Data 20-10
Viewing the Saved Packet Trace 20-11
Listing Saved Traces 20-12
Information on the Saved Trace List 20-13
Updating Packet Trace Description 20-13
Listing IP Addresses Within a Trace 20-14
Sorting IP Addresses 20-14
Locating IP Addresses 20-15
Actions on the Packet Trace IP Address List 20-16
Listing Connections Within a Trace 20-16
Sorting Connections 20-17
Locating Connections 20-17
Action on the Packet Trace Connection List 20-17
Listing Packets in a Selected Trace 20-18
Viewing Data for a Selected Packet 20-19
Viewing the Formatted Packet Display 20-21
Printing Formatted Packet Details 20-26
Errors in Packets 20-26
Dealing with Errors in Packets 20-27

Chapter 21: Connecting to Remote Hosts by Using Telnet

Using Telnet to Connect to Remote Hosts 21-2
Connecting in Full Screen Mode 21-2
Connecting in OCS Takeover Mode or Line Mode 21-2
Starting Telnet Connections 21-3
Other Methods of Starting Full Screen Telnet Connections 21-4
About the Telnet Display 21-4
Telnet Specific Function Key Assignments 21-5
Fields on the Telnet Display 21-5
Editing Text on the Telnet Display 21-5
Managing Your Telnet Connection 21-6
Searching Data on the Telnet Display 21-7
Printing from the Telnet Display 21-8
Setting Your Telnet Options 21-9
Issuing Telnet Commands 21-10
Clearing the Buffer 21-10
Hiding or Displaying the Function Key Assignments 21-10
Displaying Telnet Connection Details 21-11
Ending Your Telnet Connection 21-11
Using Line Commands to Connect to a Remote Host 21-12
Starting a Telnet Connection 21-13
Using Telnet in OCS Takeover Mode 21-13
Using Telnet in Line Mode 21-14
Automating Commands Issued to Remote Hosts 21-15
Ending a Telnet Connection in Line Mode or OCS Take-over Mode 21-15
Sending Control Codes or Special Characters to the Remote Host 21-16
Using the ---more--- Prompt 21-16

Chapter 22: Diagnosing Resources by Using SNMP

What Is SNMP? 22-2
The SNMP Standard Management Information Base (MIB) 22-2
Accessing the SNMP Functions 22-2
SNMP : Function Menu Options 22-3
Input Fields on the SNMP : Function Menu 22-4
Browsing and Changing the Value of MIB-II Objects 22-5
Accessing MIB-II 22-5
SNMP : MIB-II Access Menu Options 22-6
Browsing MIB-II Group Objects 22-7
Changing the Value of MIB-II Objects 22-8
Browsing and Changing MIB Objects by Doing a MIB Walk 22-10
Testing Connectivity 22-12
Initiating a Ping 22-12
Interpreting Responses to a Ping 22-13
Tracing a Route 22-15
Selecting a Trace Method 22-15
Initiating a Trace 22-16
Listing Managed Resources 22-18
Listing Managed Resources 22-20

Glossary

Index

Chapter

1

About NetMaster for TCP/IP

This chapter contains the following topics:

- Features and Benefits of NetMaster for TCP/IP
- TCP/IP Stack Support
- Network Scenarios and NetMaster for TCP/IP Features

Features and Benefits of NetMaster for TCP/IP

This section describes the features of NetMaster for TCP/IP and explains the associated benefits to you. The features described are:

- Management of TN3270 sessions
- Monitoring and control of FTP connections
- Logging and reporting of TCP/IP activities
- Monitoring of network events and responses
- Packet tracing for TCP/IP environments
- Monitoring of critical IP resources
  - 2216 Router and TN3270 server support
  - Cisco channel card TN3270 server support
  - Open systems adapters
  - Communications storage manager
  - Address space
  - Enterprise extender
- Web user interface
- Transaction path analyzer
- Visibility and management of SNMP
- Integrated management of multiple systems
- Real-time performance monitor
- Graphical performance manager
- Performance monitoring
- Command and resource-based security

Management of TN3270 Sessions

Help desk personnel or operators can monitor and control TN3270 sessions by using scrollable selection lists or 3270-based graphic displays of connections to remote hosts.

NetMaster for TCP/IP shows all of the hops that comprise a TN3270 connection. It uses a familiar set of TCP/IP management functions such as Trace Route, Ping, and Name Server Lookup, and extends the abilities of the NETSTAT command set to provide flexible network management capabilities. NetMaster for TCP/IP permits subsets of NETSTAT-type information such as Telnet connections for a specific address or subnet. It also provides comprehensive scroll and search capabilities.

The same general capabilities are available for the Cisco TN3270 server that resides in the Cisco channel card, for example, the Channel Interface Processor (CIP). (Some functions, like NETSTAT, are not supported by the TN3270 server.) In conjunction with NetMaster for SNA, NetMaster for TCP/IP provides a single interface to seamlessly manage the SNA and TCP/IP components of a TN3270 session.

By providing a single view of the entire TN3270 session (IP and SNA) that can be easily manipulated, problem resolution time is greatly reduced. This increases service availability, and provides assurance of service levels. The learning curve and training requirements of operation and helpdesk personnel are reduced.

Monitoring and Control of FTP Connections

NetMaster for TCP/IP provides monitoring capabilities for FTP connections to detect possible problems and take corrective action as a response. Corrective action can involve sending notifications, problem tickets, and messages, or executing a procedure to attempt to correct the problem. The product also provides scrollable selection lists and graphic displays of FTP connections. An operator can monitor the transfers, diagnose problems, locate the problem, and take corrective measures to resolve the problems. FTP client and server activity is also logged. Activity reports can be run against the logged information for better management of OS/390- or z/OS-based FTP transfers such as determining the largest FTP transfer during each eight-hour shift.

Performance is improved because a potential problem can be identified before users are affected. Operators also have a tool that allows them to monitor FTP transfers that could cause network degradation. Problem resolution is quicker because operators and helpdesk personnel have a single integrated view of the FTP transfers. Network reliability and response time increase as a result.

Logging and Reporting of TCP/IP Activities

NetMaster for TCP/IP logs all significant activities or events. This audit trail is easy to read and understand, and can be used for historical reporting purposes. NetMaster for TCP/IP records all pertinent information such as the starting and stopping of Telnet connections and FTP activity. In addition, operator commands issued, the output of those commands, and the output of executed Obeyfile are recorded. Standard reports showing TN3270 and FTP activity are provided, and sites can modify these reports or create their own from a comma-delimited file that is generated by NetMaster for TCP/IP.

This increases the diagnostic capabilities of operators and help desk personnel while greatly decreasing problem resolution time. In addition, it provides management with a concise and easy-to-understand audit trail of system activity that can be used in future network planning.

Monitoring of Network Events and Responses

NetMaster for TCP/IP provides the ability to detect significant network events, take an action, and display an alert that shows the event. This facility can check interfaces, poll devices for availability, check for listener availability, detect problems indicated by SNMP traps, detect low-level TCP/IP problems through ICMP messages, and trap system console messages indicating TCP/IP problems.

The event detection and alert monitoring facility increases network availability, reduces problems that need manual intervention (with the chance of human error). The facility reduces the need for additional help-desk or second-level support staff to resolve problems that are now detected early, and can be resolved before they cause other, perhaps more severe, problems.

Packet Tracing for TCP/IP Environments

A packet trace formatter is provided to allow full-screen views of TCP/IP packets collected by the CTRACE facility. Individual packets in a trace are displayed as an entry in the trace list. When selected, a formatted view of the packet is displayed depending on the type of packet (for example, TCP, UDP, or ICMP).

The packet trace facility saves time and increases productivity of operations personnel. It reduces the learning curve for helpdesk staff and reduces problem resolution time.

Monitoring of Critical IP Resources

NetMaster for TCP/IP provides visibility of critical IP nodes and resources.

The IP Node Monitor

The IP node monitor gives visibility to critical IP nodes such as routers. It detects when routers are not available, and can send notification, cut a problem ticket, execute a procedure, and send e-mail. Status information is maintained and the router can be queried for IP address, first hop, routing protocol, and packet size. NetMaster for TCP/IP maintains and displays hourly and daily statistics on IP path response times. For Cisco routers, additional information is provided such as CPU utilization and reliability statistics.

The IP Resource Monitor

The IP resource monitor gives visibility to the following types of critical IP resources:

- IP stacks
- Channel cards
- OSA devices
- Enterprise Extender resources
- 2216 Routers
- CSM
- Address spaces

The IP resource monitor monitors the performance of these resources and provides you with commands to manage them. These commands vary, depending on the type of resource. For example, you can browse and change the profile datasets of an IBM stack or the parameter datasets of a TCPaccess stack.

Network reliability and application availability is increased because potential resource problems that might affect users and applications can be detected earlier. Problem resolution time is decreased because technical staff has visibility of mission-critical resources and detailed information about the availability and performance in the network.

Web User Interface

NetMaster for TCP/IP provides a web browser interface to access the following functions:

- Diagnostics
- Monitoring
- Performance
- History
- Utilities

A standard user ID and password are used to access this web interface. The supported browsers are:

- Netscape Navigator (Version 4.07 or later, up to but not including Version 6.0)
- Netscape Communicator (Version 4.5 or later, up to but not including Version 6.0)
- Microsoft Internet Explorer (Version 4.01 SP 1 with JVM upgrade (5.00.3158) and Swing 1.02, or later)

The web interface can be viewed from Microsoft Windows 95, 98, and NT.

Your systems administrator can tell you the URL to use to access the web interface.

The NetMaster for TCP/IP web interface is completely OS/390 hosted. The NetMaster for TCP/IP web server runs within the NetMaster for TCP/IP address space and requires no third-party components.

Problem resolution time is decreased and ease of use increased. Help desk users who are not comfortable accessing mainframe products can diagnose problems with their standard web browser.

Every page of the web interface has context-sensitive online help.

Diagnostics

The following functions are provided on the web interface:

- IP node diagnostics
- SNA node diagnostics
- Listing Telnet connections
- Listing IP connections
- Telnet connection diagnostics
- IP connection diagnostics
- OS/390 IP stack diagnostics, including IBM TCP/IP and TCPaccess diagnostics
- Cisco channel card diagnostics
- Open Systems Adapter (OSA) diagnostics
- Enterprise Extender diagnostics
- LPD (printer) diagnostics
- Packet trace diagnostics

Monitoring

The following functions are provided:

- Alert monitoring
- IP node monitoring

Performance

The performance function is provided for the following resources:

- IP nodes
- Telnet workload
- FTP workload
- Connection workload
- OS/390 IP stacks - interface, Communications Storage Manager (CSM), and address space
- Cisco channel cards
- Open Systems Adapter (OSA) cards
- Enterprise Extender

History

The View alert history function is provided.

Utilities

The following functions are provided:

- Run a command
- View activity log
- Display region information
- Product support
- Change your password
- Logoff

Transaction Path Analyzer

NetMaster for TCP/IP provides two types of Transaction Path Analyzer to allow the real-time analysis of sessions and help you locate the source of a performance or response time problem.

Slow response time for real-time applications such as the TN3270, or poor throughput on FTP, are instances where an operator may be asked to intervene.

The two types of Transaction Path Analyzer (TPA) are:

- Telnet TPA
- Generic TPA

The initial benefit is decreased problem resolution time. Once the problem is resolved, additional benefits include increased network and application availability.

Response Time Diagnostics

The Telnet TPA provides response time information for diagnosing user-identified response time problems. The Transaction Path Analyzer is available from the Telnet connection list for displaying detailed network path analysis. This facility shows information about the network elements that are supporting the user's application access, including application, IP, and SNA information. Response time information is provided to find the point in the network path that is causing the problem, and to zoom in on the area and resolve the problem.

Throughput Diagnostics

The generic TPA monitors all non-TN3270 connections in kilobytes per second on the connection. This TPA automatically discovers the route to the node and identifies any outstanding alerts on routers in the path. FTP and logging information is provided. For example, for a completed FTP, TPA provides detailed information about user ID, IP address, byte count, and duration.

2216 Router and TN3270 Server Support

NetMaster for TCP/IP provides monitoring and control of 2216 routers and TN3270 servers. This is done by checking key device performance and utilization by interrogating the device or its available MIB variables. This facility provides performance, utilization, and session connection reports.

Cisco Channel Card and TN3270 Server Support

NetMaster for TCP/IP provides monitoring and control of Cisco channel cards such as the CIP, including connection visibility of Telnet connections with ability to select on the basis of IP address, LU name, and application name. Correlation of SNA and TCP/IP data for connections is also provided. A proprietary logging interface from the TN3270 server is used to locate information about TN3270 server status, and to optionally create alerts in the Alert Monitor.

Problem resolution time decreases as users have information in one place. Also, there are fewer training requirements because there is one standard interface for resolving problems.

Cisco Channel Card Monitor

The IP resource monitor provides proactive notification of potential problems with the CIP or CPA devices, plus the ability to track the history of usage to allow capacity planning. The feature allows the monitoring of important health indicators including:

- CPU, memory, and DMA utilization
- Transfer rates on CLAW links
- Error rates on channel interfaces
- TN3270 server users, free LU counts, and PU states

Alerts can be created when user-specified thresholds are exceeded.

TN3270 Server Support

The centralized management for multiple channel cards and TN3270 servers allows centralized monitoring of the status, configuration, and statistics related to multiple TN3270 servers. Automatic VTAM configuration diagnosis is provided so that problems can be detected and corrected. Equivalent functionality for IP connections is provided for the Cisco TN3270 server on the CIP card.

Visibility and Management of SNMP

In addition to monitoring the status of critical routers, any MIB-II compliant device can be queried, and the information returned from the device is interpreted and displayed for a help desk level user. Without this display, the user would have to understand cryptic codes and hex formats. Device information like maintenance levels and interfaces can be checked.

For more detailed MIB-II information, you can see formatted displays on various groups and subgroups within the model such as System, Interfaces, SNMP and ICMP groups, IP, UDP, and TCP subgroups. This is available for the more experienced SNMP user.

Basic usage provides the user the ability to access information and understand it without significant training efforts. For the more experienced SNMP user, the information is formatted so problem resolution time is quicker.

Integrated Management of Multiple Systems

A single logon and single screen interface provide information for managed OS/390- and z/OS-based TCP/IP regions. Additionally, NetMaster for TCP/IP allows the user to establish one or more control points over multiple OS/390- and z/OS-based TCP/IP stacks that span a single or multiple systems—for example, issuing a command to view TN3270 activity across multiple systems. This includes a mixture of both IBM TCP/IP and TCPaccess.

Centralized management for multiple Cisco channel cards and TN3270 servers is also available, providing centralized monitoring of multiple channel cards, and a centralized view of status, configuration, and statistics related to multiple TN3270 servers. In addition, a consolidated view of TN3270 sessions can be viewed for multiple channel cards and multiple OS/390-based TCP/IP stacks. Logs from other systems can be viewed from a central location from a consolidated domain panel. The log includes information from the Cisco TN3270 server, if it is being used.

Centralized management and control saves time. Consolidation of data across multiple systems is very important to ensure effective management of large sites. Without NetMaster for TCP/IP, operators have to log on to individual local and remote systems to determine the problem and issue the appropriate command.

Real-time Performance Monitor

The Real-time Performance Monitor accumulates performance data to show real-time and recent information of network utilization and performance from a 3270 interface. This helps in network usage review and network performance problem determination.

Detailed statistics, daily and hourly, are maintained on IP path response times. In addition, information from the IP node monitor provides the ability to poll and report on a range of device attributes such as:

- Router CPU time
- Router memory usage
- Interface data and error rates
- Cisco TN3270 server users and free LU counts
- Most SNMP variables

These reports include recent performance history from the IP Node Monitor, using an attribute like router CPU time. For example:

- Detailed display of the last 10 samples—can show a gradual increase in CPU time, indicating a potential problem
- Summary display of the last 24-hour period—can show peak usage for specific routers that could be balanced more efficiently

Various styles of graphs are presented, depending on the value being sampled:

- A gauge value, such as percentage CPU utilization for a router
- A rate value which represents change in a counter, for example, errors per hour
- Non-numeric values such as status values

By identifying potential device problems that could be affecting the use or attempted use of OS/390- and z/OS-based applications, the Real-time Performance Monitor has the benefit of increasing network and application reliability.

Performance Monitoring

You can enable proactive network performance monitoring through rules-based auditing and alerting of network metrics. Metrics such as IP response time and network volumes are compared against predefined utilization thresholds to generate alerts and invoke automated actions.

This feature can tie performance information directly to an alerting and automation facility in the one product by using one user interface on one platform.

Proactive notification of performance-related network events increases network reliability and availability.

Performance Data

A database repository stores both solicited and unsolicited performance data. This database allows historical reporting, network trend analysis, and capacity planning. The historical performance data is also available in a comma-delimited file or Comma Separated Values (CSV) file format to allow ODBC compliant queries and reporting.

By providing performance information, this option allows users to determine:

- Key application or device response time both in real time and historically
- TCP/IP network usage trends, application network usage, and response time
- TCP/IP stack usage and performance both in real time and historically
- Network device performance such as real-time and historical Cisco router and channel card performance

Real-time and near real-time performance information is delivered on the standard 3270 interface.

By identifying problems over time, and trends in network and application utilization, this option provides the benefits of increased network and application reliability and reduced time in real-time problem diagnosis.

Command and Resource-based Security

Four sample security levels are provided:

- Help desk ($RMSXMON)
- Network operator ($RMSXNOP)
- Operator ($RMSXOPR)
- Administrator ($RMSXADM)

For further information about the functions available to each level, see the NPF control tables ($RMSX*nnn*).

Resource checking is provided to restrict functions to particular IP address ranges—although all IP addresses are visible, the actions that can be applied are restricted.

Open Systems Adapters (OSA)

The IBM S/390 Open Systems Adapter (OSA) is a hardware device that combines the functions of a communications controller and a channel, for connecting an OS/390 or z/OS system to a network. The following tools provide visibility of OSA:

- OSA utilization
- OSA performance
- Device list for OSA
- OSA configuration

Communications Storage Manager (CSM)

The CSM manages 10 buffer pools on the OS/390 Communications Server. The monitoring of CSM buffer utilization enables you to determine the possible causes of unacceptably high CPU resource use.

Address Space

The monitoring of CPU utilization enables you to determine the possible causes of unacceptably high CPU resource use.

Enterprise Extender

The Enterprise Extender feature of OS/390 and z/OS provides high performance SNA access over an IP network. Network administrators can monitor the following areas of Enterprise Extender communications to determine if these services are available:

- The host and the lines associated with the XCA major node
- SNA sessions
- UDP ports
- Traffic through Enterprise Extender ports and availability of SNA lines to satisfy new connection requests

TCP/IP Stack Support

NetMaster for TCP/IP requires one of the following TCP/IP environments:

- IBM's eNetwork Communications Server for OS/390 V2R5 or later
- IBM's SecureWay Communications Server for OS/390 V2R8 or later
- IBM's z/OS
- TCPaccess 5.2 or later
- Cisco's IOS for S/390 Release 1.0 or later

NetMaster for TCP/IP can run in conjunction with IBM's TME 10 NetView for OS/390 or NetMaster for SNA for comprehensive network management.

Network Scenarios and NetMaster for TCP/IP Features

If you are interested in specific network scenarios and the corresponding features of NetMaster for TCP/IP to use in those scenarios, the following table serves as a guide.

In This Network Scenario...	Use These Features...
I am unable to detect and resolve TCP/IP problems prior to their impacting network functions.	Alert Monitor IP Node Monitor IP Resource Monitor Automated TCP/IP proactive monitoring, event detection, and reaction to alerts Real-time Performance Manager
I want to reduce the cost of traditional system programming staff performing first-level technical support diagnostics on IBM TCP/IP problems.	Web browser interface Integrated multiple system management TCP/IP activity log SNA to IP correlation Real-time Performance Manager

I have disparate and cumbersome tools to diagnose and resolve OS/390-based IP problems.	IP connection management Server-specific tracing TCP/IP activity log Socket programming interface Transaction Path Analyzer OS/390-based Telnet connection to remote hosts Web browser interface IP printer interface Packet trace and formatted trace displays
I lack visibility to the SNMP network from the enterprise server.	SNMP management and visibility SNMP trap generation Cisco Channel Card Monitor IP printer interface
I am unable to measure IP network usage and performance from the enterprise server.	IP Node Monitor IP Resource Monitor Real-time Performance Manager
I lack visibility of mainframe TCP/IP stack session information on distributed SNMP managers such as HP OpenView	SNMP trap generation Cisco Channel Card Monitor

Chapter

2

Getting Started

This chapter contains the following topics:

- Accessing and Leaving the NetMaster for TCP/IP Region
- Changing Your Password
- Accessing Functions
- Using Lists
- Using Data Entry Panels
- Getting Help
- Working in Two Windows

Accessing and Leaving the NetMaster for TCP/IP Region

You might have access to one or more regions. This depends on whether your organization has set up a single system or a multisystem environment.

To access the region, you must log on to it. The logon procedure is the same whether you are logging on in a single system or a multisystem environment. Before you can log on to a region, you need a user ID and password. Ensure that your system administrator has defined your user ID to the region and has allocated the relevant level of authority.

Logging On

Log on to a region as follows:

1. Enter LOGON APPLID(*acb-name*), using the ACB name of the region.
2. Enter your user ID and password on the displayed logon panel. Here is an example of the primary menu that is displayed.

```
PROD----------------- Unicenter NetMaster : Primary Menu --------------NET001
Select Option ===>

   M   - Monitors                                          Userid USER01
   H   - Historical Data                                   LU     USERF058
   D   - IP Network Diagnosis                              Time   11.16.55
   U   - User Services                                     FRI 17-AUG-2001
   O   - Operator Console Services                         OPSYS  OS390
   A   - Administration and Definition                     Window 1
   SP  - SNA Performance (Appl ID NETSPY)
   X   - Terminate Window/Exit
```

If Region Initialization Is Still in Progress

If the Initialization in Progress panel is displayed on your screen instead of the primary menu, the initialization of the region is still in progress. Press F3 (Exit) to exit to the primary menu.

The *Unicenter NetMaster Network Management for TCP/IP Implementation Guide* describes the initialization process.

If the System Image Is Still Being Loaded

If the local system image is still being loaded, the primary menu contains the **LS** option. You can select this option to monitor the loading process. You can also perform functions that do not depend on an active local image.

The *Unicenter NetMaster Network Management for TCP/IP Administrator Guide* describes system images.

Logging Off

To log out of the region, enter **=X** at the ===> prompt. This ends your current session.

If you are at the primary menu, enter **X** at the ===> prompt to end your current session.

Note: You can have two sessions for each logon to a region. If you have two sessions, repeat the procedure to end the remaining session to log off from the region.

See the section "Working in Two Windows" for details of how to use the two session windows.

Changing Your Password

Your password for logging on to a region is verified by the User Access Maintenance Subsystem (UAMS).

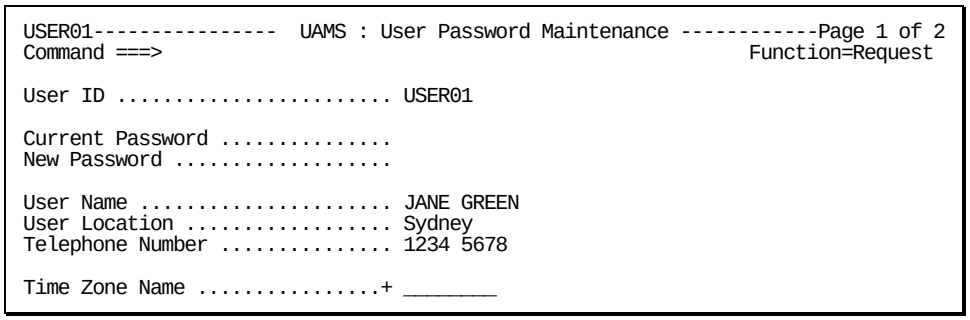
The subsystem lets you change your password, or prompts you to change your password when it has expired after a period of time. You can change your password at any time after you log on to a region. The change becomes effective the next time you log on to the region.

Note: Your installation might have linked UAMS with an external security system, such as the Resource Access Control Facility (RACF). If this is the case, your system administrator will tell you of any special considerations that apply when changing your password.

In a multisystem environment, the administrator might have set up the environment for the synchronization of UAMS user definitions and passwords. Changed passwords are then synchronized across connected regions.

Change your password to the region as follows:

1. Enter **/CHGPWD** at a ===> prompt to access the panel that enables you to change your password. The User Password Change panel is displayed.



   Note: You can press F12 (Cancel) to cancel the operation at any time before Step 3.

2. Type your current password in the Current Password field, and your new password in the New Password field. These fields do not display the entered information.

   You are prompted to retype your new password for confirmation.

3. Press F3 (File) to file the changed password.

   If an error message is displayed indicating that an entered password is incorrect, repeat from Step 2.

   If UAMS synchronization is enabled, a Linked Regions UAMS Update Report panel is displayed when you save your changed password. The panel reports the success or failure of the password change in the connected regions.

   If synchronization fails, ask the administrator to reset your password when the problem is corrected.

Authority Levels

If you have access to NetMaster for TCP/IP you have monitoring authority. Additional authority is required to:

- Execute an obeyfile
- Use packet tracing
- Start and stop devices
- Drop connections
- Add and update SNMP manager records
- Change the value of MIB-II objects

If you attempt to issue an unauthorized command, an error message is displayed, telling you that you are not authorized to perform that function. See the *NetMaster for TCP/IP Administrator Guide* for details on setting up security.

Accessing Functions

You access functions in the region through the user interface menus by doing one of the following:

- Selecting an option from each menu that leads to the function
- Specifying the shortcut to go to the function directly
- Specifying the path to go to the function directly

Selecting an Option

You select an option by entering the option code at the ===> prompt. For example, entering **A** at the ===> prompt on the primary menu takes you to the Administration primary menu.

Selecting a Function Directly—Using Shortcuts

You can jump to the panel of a function directly by using shortcuts. You can specify the shortcut at a ===> prompt in one of the following ways:

- Specify ***/shortcut-name*** to retain the current panel on return.
- Specify ***=/shortcut-name*** to close the current panel and return to the primary menu on exit.

Each entry on a menu may be followed optionally by a shortcut, displayed in turquoise. If you do not remember a shortcut, enter / or =/ to list the shortcuts and then select one.

Accessing a Function by Using */shortcut-name*

Important! *If your current panel does automatic updates and you no longer need this information, use =/shortcut-name rather than a nested shortcut. This saves storage and resources because the region does not need to maintain a display that you no longer need.*

To select the function you want, enter its corresponding shortcut, preceded by the slash (/) character, at a ===> prompt.

For example, to access the Resource Administration menu, enter **/RADMIN** at the ===> prompt on your current panel. When you have finished with the menu, press F3 to redisplay your previous panel.

When you access a function by using its shortcut, your current panel is retained. When you press F3 to exit out of the function, this panel, with any updates, is restored. By using shortcuts, panels can be nested to a maximum of 64 levels.

Accessing a Function by Using =/*shortcut-name*

Whenever you have finished with your current panel, you can access the next function by prefixing the shortcut call with the equals (=) sign. This goes directly to the function without retaining the current panel and closes all other nested panels in this window.

For example, to access the Resource Administration menu without retaining the current panel, enter **=/RADMIN** at the ===> prompt on your current panel. When you have finished with the menu, press F3 to display the primary menu.

Selecting a Function Directly—Skipping Panels

You can jump to the panel of a function directly by specifying the exact path to that panel. Construct the path by linking the options you need with periods. Depending on which panel you start from, you specify the panel path in one of the ways described in the following sections.

Accessing a Panel That Is Lower in the Panel Hierarchy

If you start from a menu and want to access a panel lower in the panel hierarchy, specify the path as it is. For example, if you are at the primary menu and want to change your password, type **U.P** at the ===> prompt and press ENTER.

Accessing a Panel That Is Higher in the Panel Hierarchy

If you want to access a panel that requires you to pass through a panel higher up in the panel hierarchy, you must precede the path specification with the equals sign (=). The = character brings you back to the primary menu and then to the required panel. You can specify such a path at any ===> (or =>) prompt. For example, if you are at Resource Definition panel and want to change your password, enter **=U.P** at the ===> prompt and press ENTER.

To return to the primary menu, enter **==**.

Accessing a Panel That Requires Input Data

If you want to access a panel that requires you to enter data, you can enter the data by separating them from the path by a semicolon (;). For example, if you are at the primary menu and want to access the IP resource monitor for the linked region PROD2, type **M.I;PROD2** at the ===> prompt and press ENTER.

Using Lists

Lists comprise a series of items from which you can make a selection, or against which you can perform actions. The fourth line on a panel describes the actions that can be performed on the listed items.

Here is an example of a list.

```
PROD------------------ TCP/IP : Telnet Connection List ------------Link: PROD02
Command ===>                                                    Scroll ===> PAGE

 Line 1 of 9                          Refresh Every ... ___  Seconds
 P=Ping T=TraceRoute D=VTAM Display SL=Session List NL=Lookup S=View Z=Drop
               I=Information TPA=Transaction Path Analyzer L=Log ?=Actions
                                                        Bytes    Bytes
    Foreign Host    LU Name  Applname Status             Out       In
    123.0.12.30     SDTCP006 TEST1    Establsh       115565    20514
    123.0.11.23     SDTCP002 TEST1    Establsh        36128      252
    123.123.123.85  SDTCP001 TEST4    Establsh       998114   106077
    123.0.123.33    SDTCP007 TEST1    Establsh        60757     9786
    123.0.11.22     SDTCP004 TEST1    Establsh        49806    11874
    123.0.123.53    SDTCP003 TEST1    Establsh       651908    45035
    123.0.12.34     SDTCP005 TEST1    Establsh        76398     1030
    123.123.123.86  SDTCP008 TEST4    Establsh         9892      277
    123.123.2.34    SDTCP009 TEST1    Establsh        15456      500
    **END**
```

There are four different types of list:

- Action lists—allow you to apply *actions* to one or more listed items. Enter the required action code beside the appropriate records.
- Single select lists—allow you to select one item from a list (for example, the list of valid values for a data entry field) by:
  - Entering the **S** (Select) action code beside the item
  - Moving the cursor to a position anywhere in the line containing the item you want to select and pressing ENTER
- Multiple select lists—allow you to select one or more items in a list (for example, the list of panels that you use to customize your user profile).
- Numbered lists—allow you to select a single item from the list by entering the appropriate number at the ===> prompt (for example, the list of valid values for a data entry field).

If a list is longer or wider than one panel, you can scroll vertically or horizontally, as appropriate.

Scrolling

When the listed information cannot fit onto the screen, use scrolling to access the off-screen information. You can scroll vertically and horizontally.

Scrolling Vertically

Use the F8 (Forward) or F7 (Backward) function key to scroll the displayed information forward or backward by the amount displayed at the Scroll ===> prompt. The following table shows the valid scroll amounts.

Scroll Amount	Action
C (or CSR)	If scrolling forward, the line on which the cursor is currently positioned is moved to the top of the screen. If scrolling backward, the line on which the cursor is currently positioned is moved to the bottom of the screen.
D (or DATA)	The display is scrolled one full page, less one row, in the specified direction. If scrolling forward, the last line of the current page is displayed as the first line on the next page. If scrolling backward, the first line on the current page is displayed as the last line on the next page.
H (or HALF)	The display is moved half a page in the specified direction.
M (or MAX)	The display is moved to the beginning or the end of the displayed information, depending on the function key (Forward or Backward) used.
P (or PAGE)	The display is moved one full page in the specified direction.
n	The display is moved *n* lines in the specified direction.

You can also enter a temporary scroll amount at the Command ===> prompt (for example, Command ===> 5). When you press the F7 (Backward) or F8 (Forward) function key, the displayed information is scrolled by the specified value once *only*.

Scrolling Horizontally

Use the F11 (Right) or F10 (Left) function key to scroll the displayed information to the right or to the left.

Searching for an Item in Retrieved Information

You can search for specific items in the retrieved information by using the F5 (Find) function key or the LOCATE command.

Using the F5 (Find) Function Key

The F5 (Find) function key enables you to find a particular occurrence of text in the retrieved information. Enter the text you want to find, and press F5. If the text contains more than one word, enclose the text in quotation marks.

You can press F5 again to find the next instance of the text.

You can enhance the Find function in the following ways:

- Expand the search beyond the columns currently displayed by using the FMODE command
- Change the number of records searched between prompts by using the FPROMPT command

For information about the FMODE and FPROMPT commands, see Help.

Using the LOCATE Command

The LOCATE command enables you to locate a particular record in a list. Enter **LOCATE** or **L** followed by a text string mask. The command locates the first record name that matches the mask.

Using Data Entry Panels

Each record in the knowledge base is displayed and maintained through a sequence of panels on which you enter the data for that record.

Switching to UPDATE Mode

Many definition panels enable authorized users to switch from the BROWSE mode to the UPDATE mode by pressing F4 (Edit). You can then edit the displayed information.

Entering Data

On a color screen, mandatory fields that you must complete are colored white. Optional fields, which you can complete as and when required, are colored turquoise. Both types of fields can be prompted fields that provide you with a list of valid values, from which you can choose one.

Prompted Fields with a List of Valid Values

Many fields on the data entry panels are linked to lists containing the values that you can choose for the field. These fields are called prompted fields. Most, but *not* all, prompted fields are identified by a plus sign (+).

Enter **?** in a prompted field to display the value list, which could be either a numbered list or a single select list.

You can prefix the question mark (?) with one or more characters. The displayed list is then restricted to values that start with those characters. For example, enter **S?** to display a list of values that start with S.

Validating and Filing Data

During data entry, you can press ENTER to validate your data. Validation also occurs when you try to:

- Access another panel (for example, when you press F8 (Forward) to access the next panel)
- Save your entered data (for example, when you press F3 (File) to save a definition)

When you have finished entering data, you can do one of following:

- Press F3 (File) to save the data and exit the panel.
- Press F4 (Save) to save the data and remain on the panel. When adding definitions, this enables you to quickly create other similar definitions, minimizing the typing required.
- If you do *not* want to save the data, press F12 (Cancel) to exit the panel.

Moving Between Panels

Some functions lead to a series of data entry panels (for example, when you update a resource definition).

You can use one of the following methods to move through these panels, depending on what you need to do.

Selecting All Panels

You might want to access every panel. All the panels are listed on a Panel Display List panel (for example, the panel that lists the resource definition panels). Enter **S** beside the name of the panel you want to access first, or enter the number that identifies that panel in the panel sequence at the Command ===> prompt (for example, 1 for the first panel). The selected panel is displayed.

Press F8 (Forward) to scroll forward to the next panel; press F7 (Backward) to scroll backward to the previous panel.

When you finish entering the data, press F3 (File) to save the data. Press F12 (Cancel) if you decide not to save the data.

Selecting Specific Panels from the Panel Display List

You might want to access certain panels only (for example, when you want to update only certain parts of a resource definition). All the panels required for a definition are listed on a Panel Display List. Type **S** beside the names of the panels you want to access. Once you have made all your selections, press ENTER to display the first panel you selected. Then press F8 (Forward) to scroll forward through the panels you selected. Press F7 (Backward) to scroll backward through the panels you selected.

When you finish entering the data, press F3 (File) to save the data. Press F12 (Cancel) if you decide not to save the data.

Selecting a Panel from Another Panel

If you want to skip to a panel that is not next in the sequence, and you know the sequence number of the panel you want, enter that number at the Command ===> prompt. The required panel is displayed.

Selecting a Panel from the Index Menu

From some data entry panels, you can press F11 (Panels) to display the Index Menu panel. This menu lists all the panels available for that function. Use the Index Menu if you want to jump to a panel but do not know its place in the panel sequence.

Note: If you have selected two or more panels previously, pressing F11 (Panels) displays a list of the selected panels only. You can press F6 (AllPanel or SelPanel) to switch between the full list and the partial list.

Saving a Sequence of Definition Panels for Repeated Access

On a definition list panel, you can select more than one definition. You can then work on the selected definitions in sequence. Each definition can contain a number of definition panels. Normally, the list of panels is displayed on your screen for you to select each time you access a new definition. However, if you want to browse or update the same panels for each selected definition, you can save the list of panels you want, as shown in the following procedure.

As you move through the sequence of selected definitions, the panels appear on your screen according to the saved list. You do *not* have to select the panels again when you move on to the next definition.

The following procedure uses the resource definition panels as examples:

1. Enter the **/RADMIN.R.ASMON** path to access the list of address space definitions. The Address Space Monitor List panel is displayed.
2. Type **B** (Browse) or **U** (Update) next to the definitions you want to access. You can use the F7 (Backward) or F8 (Forward) function keys to scroll through the list.
3. Press ENTER to select the definitions. The Panel Display List window is displayed, listing the resource definition panels.
4. Type **S** next to the panels you want, and press F4 (SaveSeq) to save the list of selected panels.
5. Press ENTER to bring up the first selected panel.

When you finish with one group definition, the panels for the next definition are displayed in the same sequence.

Getting Help

Online help is provided for panels and messages.

Online help is context-sensitive and available at different levels. When you are viewing a help panel, pressing F1 (Help) takes you to the next level of help available. Pressing F3 (Exit) takes you back to the previous level of help, or exits from help and returns you to the application. Pressing F4 (Return) exits help and returns you to the application immediately.

Using the Tip of the Day

The region displays a tip about using the product at the bottom of the primary menu. To display the detailed tip, place the cursor on the tip and press F1 (Help).

Getting Help About a Panel

Panel-based online help includes information about what each panel is used for, how to complete the fields, the actions you can perform, and the use of available function keys. Use this online help to supplement the information in this guide while you are working in the region.

Press F1 (Help) to retrieve the online help for a given panel. When you are viewing a help panel, you can press F6 (HelpHelp) to find out how to use the help facility.

If the block of help text you require splits across two panels, use the arrow keys to move the cursor to the top or the bottom of the block and press F8 (Forward) or F7 (Backward) to bring the block into view.

Getting Help About a Message

While you are working in the region, you receive messages that advise you of various events. These messages might be providing information only (for example, informing you that an update has been successful). They might also alert you to errors (for example, if you try to enter an action that is not valid for a resource).

Each message has detailed online help text associated with it. Access the help text for a particular message in one of the following ways:

- If you are viewing a transient log, enter **H** beside the message.
- If you are at a panel and a message is displayed in red on the third line of that panel, move the cursor to that line and press F1 (Help).
- If you receive a message referring you to the activity log for more detail, enter **/LOG** at the ===> prompt to display the activity log. For details about the activity log, see the *Management Services User's Guide*.
- If you are using the activity log, a Command Entry panel, or OCS, you can do one of the following:
  - Move the cursor to the line displaying the message, and press F1 (Help).
  - Type the message ID at the => prompt, and press F1 (Help).
- You can also enter **/CODES** to display the Messages and Codes Menu panel that enables you to obtain help on messages and on miscellaneous error codes.

Working in Two Windows

You can divide your physical screen into two logical windows. Each window operates independently of the other, enabling you to perform multiple functions concurrently. For example, you can access the IP resource monitor in one, and an OCS window in the other.

You can open a second window anywhere in the NetMaster for TCP/IP region by using the F2 (Split) or F9 (Swap) function keys. When one window takes up the entire screen, the other window is termed *closed*.

Splitting Screens

Using the SPLIT command, you can:

- Split your screen horizontally and have one window above the other—move the cursor to a row where you want to split screens, and press F2 (Split).
- Split your screen vertically and have two windows side by side—move the cursor to any column on the bottom row, and press F2 (Split).

Swapping Screens

Using the SWAP command, you can:

- Reverse the dimensions of the active window, if you have two windows open and both are visible on the screen, and toggle between them
- Open a second full-screen window, if you are currently operating with a single window open, and then toggle between them

To toggle between two full-screen windows:

1. Decide which two panels you want to toggle between and display one of them.
2. Press F9 (Swap) to display the primary menu.
3. Proceed to the second panel you require and press F9 (Swap). The first of your swap-panels is redisplayed.
4. Press F9 (Swap) to toggle between the two swap-panels.

Chapter

3

Managing Connections

This chapter contains the following topics:

- About Connection Lists
- Listing Telnet Connections
- Listing CICS Socket Connections
- Listing General Connections
- Displaying Connection Information
- Displaying Connections Graphically
- Displaying Status of TCP/IP Resources
- Listing Specific Connections

About Connection Lists

From a connection list you can diagnose performance or connectivity related problems. For example, if an FTP file transfer is taking an unusually long time or is stalling, you may want to view the connection information to see if there are any data transfer problems. You could then apply the TPA (Transaction Path Analysis) action or TraceRoute action, using the time taken for responses, to see where along the route the data transfer problems are occurring.

You can produce a list of connections to the IBM TCP/IP (or TCPaccess) host or Cisco channel card to match a set of criteria. For example, you can produce a list specifically for all Telnet connections or, more generally, for all connections with a particular task name. You can also produce a list of all connections with a particular local port number.

For more information about testing connectivity with the Ping action or using the TraceRoute action, see Testing Connectivity and Tracing a TCP/IP Route in the chapter “Diagnosing Connection Problems”.

Types of Connection Lists

To see the types of connections that you can list, enter **/IPCON** at a ===> prompt. The TCP/IP : Connections menu is displayed.

TCP/IP : Connections Menu

```
PROD----------------------- TCP/IP : Connections ----------------------/IPCON
Select Option ===>

   T   - List Telnet Connections                          CONNTEL
   TRS - List Telnet Connections - with Response Times    CONNTRS
   TRT - List Telnet Connections - with Round Trip Times  CONNTRT
   CS  - List CICS Socket Connections                     CONNCS
   CSH - List CICS Socket Connections - with History      CONNCSH
   C   - List Connections                                 CONNT
   CF  - List Connections - Fast                          CONNTF
   CH  - List Connections - with History                  CONNTH
   X   - Exit
```

The three basic types of connection that you can list are:

- Telnet connections
- CICS socket connections
- General connections

Within these basic types, you can choose different options from the menu to view various levels of detail.

Availability of Connection Lists

Option TRS is available only if the NetSpy Agent is currently active in your region.

Options CS and CSH are available only if your region is configured with the NetMaster Socket Management for CICS product.

Connection List Criteria

For each of the three basic types of connection, there is a Connection List Criteria panel. This is displayed when you select an option and it allows you to specify criteria to filter the connections to be displayed. You can also store your specified criteria so that you can recall them at any time instead of having to enter them again.

TCP/IP : Telnet Connection List Criteria

```
PROD-------------- TCP/IP : Telnet Connection List Criteria --------------------
Command ===>                                                  Function=Search

Connection List Criteria
  Remote Host .......... ____________________________________________________
  Telnet LU Name ....... ________
  Telnet Application ... ________________________________
  Link/Channel Card ...+ ________________________

Store and Recall Criteria
  Criteria Name .......+ ___________


 F1=Help      F2=Split     F3=Exit                 F5=Recall    F6=Action
                           F9=Swap                F11=Store
```

Specifying Criteria

To list connections by one or more criteria:

1. Enter values in the relevant Connection List Criteria fields.
2. Press F6 (Action). A connection list is displayed, satisfying the criteria that you specified.

Note: The last criteria that you used for a given type (Telnet, CICS, general) are stored in your profile record and are automatically displayed when you access a connection list criteria panel.

Storing Criteria

To define and store criteria for future use:

1. Enter values in one or more of the Connection List Criteria fields.
2. Enter a value in the Criteria Name field to identify this set of criteria.
3. Press F11 (Store). The TCP/IP : Save Connection List Search Criteria panel is displayed.

TCP/IP : Save Connection List Search Criteria

```
PROD-------------TCP/IP : Save Connection List Search Criteria-----------------
Command ===>                                                    Function=Add

  Criteria Type ....+ List Connections

  Criteria Name ....+ __________

  Description ....... ____________________________________________________________

  Replace? .......... NO_  (Yes/No)


 F1=Help      F2=Split     F3=File      F4=Save
                           F9=Swap                              F12=Cancel
```

4. Enter values in the input fields.
5. Press F4 (Save) to store the specified criteria in the Virtual File Services (VFS) dataset.

Recalling Criteria

To list connections satisfying a stored set of criteria:

1. Enter a value in the Criteria Name field.

   Note: To display a selection list of stored criteria names, enter **?** in the Criteria Name field. When you select an entry from the list, NetMaster for TCP/IP uses the stored criteria definition to complete the Connection List Criteria fields.

2. Press F6 (Action). A connection list is displayed, satisfying the stored criteria that you specified.

Listing Connections for Multiple Systems

The connection lists display information about the current state of active connections to multiple host systems. Connection lists for multiple systems are available for the following types of systems:

- Multiple IBM TCP/IP hosts
- Multiple TCPaccess hosts
- Multiple channel cards or 2216 routers
- Mixed hosts including IBM TCP/IP hosts, TCPaccess hosts, and Cisco channel cards.

Note: Channel cards and 2216 routers are available for selection from the Telnet connection list only.

Multiple-system connection lists can be particularly useful if you are migrating users from one type of access to another.

To display a list of connections for multiple systems, do this on the appropriate Connection List Criteria panel:

1. Enter **?** in the Link/Channel Card field or the TCP/IP Stack field to display a selection list of link names or stacks.
2. Select the host systems whose connections you want to list and press ENTER.

   The Connection List Criteria panel is displayed with *MULTIPLE* in the Link/Channel Card field or the TCP/IP Stack field.
3. Press F6 (Action).

   The connection list is displayed with the words LINK: *MULTIPLE* at the top right corner of the panel. The link for each connection is shown in the Link Name column.

Sorting Connection Lists

The SORT command allows you to display connections in a specific order.

The only operand is the column heading of the column you wish to sort by. For example, enter SORT Status to sort the list by Status. The minimum number of characters needed to uniquely specify the column is sufficient. For example, SORT F is equivalent to SORT Foreign Host.

To sort by other than the set default value, do this:

1. At the ===> prompt, enter **SORT ?**. The Sort Values List is displayed, allowing you to select any of the listed values.
2. Select the sort value that you want, and press ENTER. The appropriate connection list is displayed, sorted in the specified order.

Note: For Telnet connection lists, a system-wide default sort order can be set, by using the TELNETLISTS parameter group in ICS. For more information, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

Locating Information on Connection Lists

You can use the LOCATE command to position a connection list to a particular row on the list.

This command is available only on sorted connection lists. For information about sorting the list by using the SORT command or (for Telnet connection lists only) by setting a system-wide default, see the section “Sorting Connection Lists”.

The value you specify after the LOCATE command applies to the sort value that applies to the list. It does not necessarily apply to the first column of the list unless you have sorted by the first column.

Examples

If you have sorted by foreign host and you issue the LOCATE 200 command, the cursor is positioned at the line before the first IP address that starts with 200.

If you have sorted by status and you issue the LOCATE Listen command, the cursor is positioned at the line before the first status that starts with Listen.

Listing Telnet Connections

The Telnet Connection List displays information about the current state of active Telnet connections to this IBM TCP/IP host (or TCPaccess host) or Cisco channel card or 2216 router.

Telnet Connection List Criteria

To display the Telnet Connection List Criteria panel:

1. Enter **/IPCON** at a ===> prompt. The TCP/IP : Connections menu is displayed.
2. Enter one of the three Telnet options (T, TRS, or TRT) at the ===> prompt. The TCP/IP : Telnet Connection List Criteria panel is displayed.

TCP/IP : Telnet Connection List Criteria

```
PROD-------------- TCP/IP : Telnet Connection List Criteria -------------------
Command ===>                                                  Function=Search

Connection List Criteria
  Remote Host .......... ____________________________________________________
  Telnet LU Name ....... ________
  Telnet Application ... ____________________________
  Link/Channel Card ...+ ________________________

Store and Recall Criteria
  Criteria Name .......+ ___________


 F1=Help      F2=Split     F3=Exit                 F5=Recall    F6=Action
                           F9=Swap                F11=Store
```

3. To list Telnet connections by one or more criteria, complete the relevant Connection List Criteria fields or the Criteria Name field and press F6 (Action).

Telnet Connection List

To display the Telnet Connection List, press F6 (Action) from the Telnet Connection List Criteria panel.

TCP/IP : Telnet Connections (with Round Trip Times)

```
PROD------------------ TCP/IP : Telnet Connections ----------------------------
Command ===>                                                  Scroll ===> CSR

    Line 1 of 9                                  Refresh Every ... ____ Seconds
     SL=Session List D=VTAM Display P=Ping T=TraceRoute NL=Lookup S=View Z=Drop
                   I=Information TPA=Transaction Path Analyzer L=Log ?=Actions
                             Appl                    Total           RTT  ReXmit
    Foreign Host    LU Name  Name     Status        Bytes   RTT      Var   Count
    155.35.212.138  SSTCP001 STNM1    Establsh     711018   284       18      11
    141.202.145.93  SSTCP019 STNM4    Establsh      26174   114       94       0
    155.35.122.113  SSTCP003 STNM1    Establsh     444623   345       25      31
    155.35.122.140  SSTCP034 STNM1    Establsh     200409   400       80      28
    155.35.122.140  SSTCP035 STNM1    Establsh     134713   401       59      23
    155.35.122.140  SSTCP037 STNM1    Establsh      68479   407       77      23
    155.35.122.168  SSTCP039 STNM1    Establsh     403839   341       24      10
    155.35.122.138  SSTCP047 STNM1    Establsh    1849923   350       10      44
    155.35.212.138  SSTCP002 STNM1    Establsh     335290   282       12       1
    **END**
```

The Telnet Connection List can provide the following types of information:

- Mapping of IP addresses to LU names and application names
- Combined information from more than one of these sources—IBM TCP/IP, TCPaccess, or the channel card

To investigate problems occurring on any of the listed connections, use the actions shown on the TCP/IP : Telnet Connection List panel (for example, P=Ping or T=TraceRoute).

Columns on the Telnet Connection List

For information about the information displayed on the Telnet Connection List, press F1 (Help).

Actions and Commands on the Telnet Connection List

For information about the actions and commands available on the Telnet Connection List, press F1 (Help).

Note: Some actions are available for particular connections only. For example, the Mini Trace action is available from a Telnet connection list for a channel card only.

Listing All Actions on the Telnet Connection List

To display a selection list of all the actions you can apply on the Telnet Connection List, enter **?** next to the connection to which you want to apply an action. The following panel shows a selection list of actions on the Telnet Connection List.

```
PROD-------------- TCP/IP : Telnet Connection List Actions --------------------
Command ===>                                                  Scroll ===> CSR

                         Use 'S' to select the required Connection List action
    Action Description                                 Restrictions
    BT     Buffer Trace
    BTC    Buffer Trace Clear
    D      VTAM Display
    I      Information
    L      Display Activity Log
    MT     Mini Trace                                  Channel Card only
    NL     Name Lookup
    P      Ping
    PT     Packet Trace
    PTC    Packet Trace Clear
    S      View Connections Display
    SL     Session List
    ST     SNA Trace
    STC    SNA Trace Clear
    T      TraceRoute
    TPA    Transaction Path Analyzer
    V      View Connections Display
    Z      Drop Connection
    **END**
```

Listing CICS Socket Connections

The CICS Socket Connection List displays information about the current state of any active CICS socket connections.

CICS Socket Connection List Criteria

To display the CICS Socket Connection List Criteria panel:

1. Enter **/IPCON** at a ===> prompt. The TCP/IP : Connections menu is displayed.

2. Enter one of the two CICS Socket Connections options (CS or CSH) at the ===> prompt. The TCP/IP : CICS Socket Connection List Criteria panel is displayed.

TCP/IP : CICS Socket Connection List Criteria

```
PROD----------- TCP/IP : CICS Socket Connection List Criteria -----------------
Command ===>                                                  Function=Search

Connection List Criteria
  Remote Host ........ ____________________________________________________
  Remote Port ........ ________
  Local Port ......... ________
  CICS Tran ID ....... BBAL
  CICS Terminal ...... ________
  Task Name .......... ________
  User ID ............ ________
  TCP/IP Stack ......+ ____________

Store and Recall Criteria
  Criteria Name .....+ __________
```

3. To list connections by one or more criteria, complete the relevant Connection List Criteria fields or the Criteria Name field and press F6 (Action).

   For example, to list connections by CICS region, complete the Task Name field. To list connections by CICS transaction ID, complete the CICS Tran ID field.

CICS Socket Connection List

To display the CICS Socket Connection List, press F6 (Action) from the CICS Socket Connection List Criteria panel.

TCP/IP : CICS Socket Connections (with History)

```
PROD-------------- TCP/IP : CICS Socket Connections (hist) --------------------
Command ===>                                                 Scroll ===> CSR

    Line 1 of 22                                  Refresh Every ...      Seconds
                 DC=Display CICS P=Ping T=TraceRoute NL=Lookup S=View Z=Drop
       ZC=Drop CICS I=Information TPA=Transaction Path Analyzer L=Log ?=Actions
                  Remote Local                        CICS Transaction   CICS
    Foreign Host     Port  Port User ID  TaskName  ID   Task Number   Terminal
    123.200.110.136  2605  2657 -        PROD4     BBAL 00260080      LT01
    123.200.109.49   2711  2650 -        PROD6     BBAL 00260080      LT01
    123.200.109.49  20049  2706 -        PROD6     BBAL 00260080      LT01
    123.35.122.67    2636  2643 -        PROD4     BBAL 00260080      LT01
    123.35.222.14    1586    23 -        TCPIP3    BBAL 00260080      LT01
    123.200.110.194 65535  2566 -        PROD6     BBAL 00260080      LT01
    123.35.122.163   2460    23 -        TCPIP3    BBAL 00260080      LT01
    123.35.106.93    1116    23 -        TCPIP3    BBAL 00260080      LT01
    123.35.122.136   1309    23 -        TCPIP3    BBAL 00260080      LT01
```

Columns and Actions on the CICS Socket Connection List

To view all of the information on this panel, press F11 to scroll right. For details of the information displayed, press F1 (Help).

Listing All Actions on the CICS Socket Connection List

To display a selection list of all the actions you can apply on the CICS Socket Connection List, enter **?** next to the connection you want to apply an action to. The selection list is displayed.

```
PROD---------- TCP/IP : CICS Socket Connection List Actions -------------------
Command ===>                                                  Scroll ===> CSR

                         Use 'S' to select the required Connection List action
    Action Description                                 Restrictions
    DC     Display CICS Socket Information
    I      Information
    L      Display Activity Log
    NL     Name Lookup
    P      Ping
    PT     Packet Trace
    PTC    Packet Trace Clear
    S      View Connections Display
    T      TraceRoute
    TPA    Transaction Path Analyzer
    V      View Connections Display
    Z      Drop Connection
    ZC     Drop CICS Socket Connection
    **END**
```

For information about the actions and commands available on the CICS Socket Connection List, press F1 (Help).

Listing General Connections

The Connection List displays information about the current state of any active connections to the selected stack. You can investigate problems occurring on any of the listed connections by using the actions shown on the Connection List panel. This is particularly useful if you are investigating problems in FTP connections.

Connection List Criteria

To display the Connection List Criteria panel:

1. Enter **/IPCON** at a ===> prompt. The TCP/IP : Connections menu is displayed.
2. Enter one of the three Connections options (C, CF, or CH) at the ===> prompt. The TCP/IP : Connection List Criteria panel is displayed.

TCP/IP : Connection List Criteria

```
PROD----------------- TCP/IP : Connection List Criteria -----------------------
Command ===>                                                  Function=Search

Connection List Criteria
  Remote Host ........ ____________________________________________________________
  Remote Port ........ ________
  Local Port ......... ________
  Application Name .... ____________________________
  Task Name ..........  INT*____
  LU Name ............ ________
  User ID ............ ________
  TCP/IP Stack .......+ ________________________

  Store and Recall Criteria
  Criteria Name .......+ ___________
```

3. To list connections by one or more criteria, complete the relevant Connection List Criteria fields or the Criteria Name field and press F6 (Action).

   For example, to list connections by task, complete the Task Name field—it should contain an appropriate full task name (for example, INTCLIEN) or a task name mask (for example, FTP*) for the task or tasks on your system. To list connections by user ID, complete the User ID field.

Connection List

To display the Connection List, press F6 (Action) from the Connection List Criteria panel.

TCP/IP : Connections (with History)

```
PROD-------------------- TCP/IP : Connections (hist) -----------Stack: IBMTCPIP
Command ===>                                                 Scroll ===> PAGE

Line 1 of 28                                    Refresh Every ...____ Seconds
                                      P=Ping T=TraceRoute NL=Lookup S=View Z=Drop
                  I=Information TPA=Transaction Path Analyzer L=Log ?=Actions
    Foreign Host     Port Local Host       LPort LU Name  User ID  TaskName
    10.0.123.41      1460 10.123.4.31         23                   INTCLIEN
    10.0.123.36      1088 10.123.4.31         23                   INTCLIEN
    10.123.1.126     1033 10.123.4.31         23                   INTCLIEN
    10.123.4.31      1032 10.123.4.31         23                   INTCLIEN
    10.123.4.31      1033 10.123.4.31         23                   INTCLIEN
    10.123.4.31      1034 10.123.4.31         23                   INTCLIEN
    10.123.4.51      1049 10.123.4.31         23                   INTCLIEN
```

Columns and Actions on the Connection List

To view all of the information concerning connections on this panel, press F11 to scroll right. For details of the information displayed, press F1 (Help).

Listing All Actions on the Connection List

To display a selection list of all the actions you can apply on the Connection List for a task, enter **?** next to the connection you want to apply an action to. The selection list is displayed.

```
PROD----------------- TCP/IP : Connection List Actions ------------------------
Command ===>                                                  Scroll ===> CSR

                        Use 'S' to select the required Connection List action
    Action Description                                 Restrictions
    I      Information
    L      Display Activity Log
    NL     Name Lookup
    P      Ping
    PT     Packet Trace
    PTC    Packet Trace Clear
    S      View Connections Display
    T      TraceRoute
    TPA    Transaction Path Analyzer
    V      View Connections Display
    Z      Drop Connection
    **END**
```

For information about the actions and commands available on the Connection List, press F1 (Help).

Displaying Connection Information

To display the Connection Information panel, enter **I** next to a connection on a connection list. The Connection Information panel is displayed.

```
PROD-------------------- TCP/IP : Connection Information --------------------
Command ===>

Remote IP Address .... 123.123.12.234
       Port Number ... 1030
Via Router ........... 123.123.12.21
Connection State ..... Connected
           ID ........ 207
Idle Time ............ 00:00:03
Connection Duration .. 01:04:11
ACB Name ............. ACCVLT03
Application Name ..... TEST1

Statistics                          Sent             Received
Segments ........................... 304              283
Bytes .............................. 147216           918
Retransmissions .................... 17728            0
TCP Window Size .................... 8538             0
Leftmost Sequence Number ......... 527388           122219177
Average Round Trip Time (RTT) .... .75              N/A
Deviation Round Trip Time (DEV) .. .20              N/A
```

The Connection Information panel displays details of the selected connection. For details of the information displayed, press F1 (Help).

Displaying Connections Graphically

The connections from a particular remote host can be graphically displayed from a connection list.

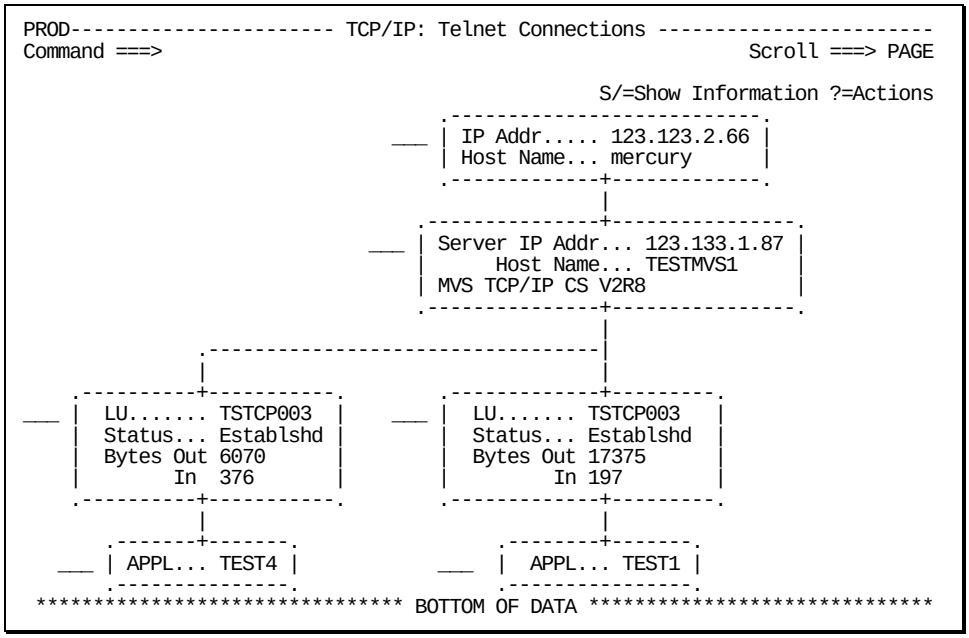
As for a connection list, you can diagnose performance- or connectivity-related problems from a graphical display.

If there are no active connections of the requested type between TCP/IP and the remote host, only the remote IP host and TCP/IP host boxes are shown on the graphical display. NetMaster for TCP/IP automatically pings the remote host to determine whether or not a path exists. If the ping fails, the line connecting the boxes flashes red.

Displaying Telnet Connections

To present the Telnet Connections display for a specific Telnet host, enter **S** next to an entry on the Telnet Connection List. The Telnet Connections panel is displayed.

Telnet Connections Display



The Telnet connections display has four layers: the TCP/IP host, the Telnet server, the connection(s), and the SNA application(s).

Once the display splits out at the third layer to show connections, you cannot rejoin it at the application level, even if the same application is being used. This enables the different application sessions to be distinguished.

Fields and Actions on the Telnet Connections Display

For information about the display fields, press F1 (Help).

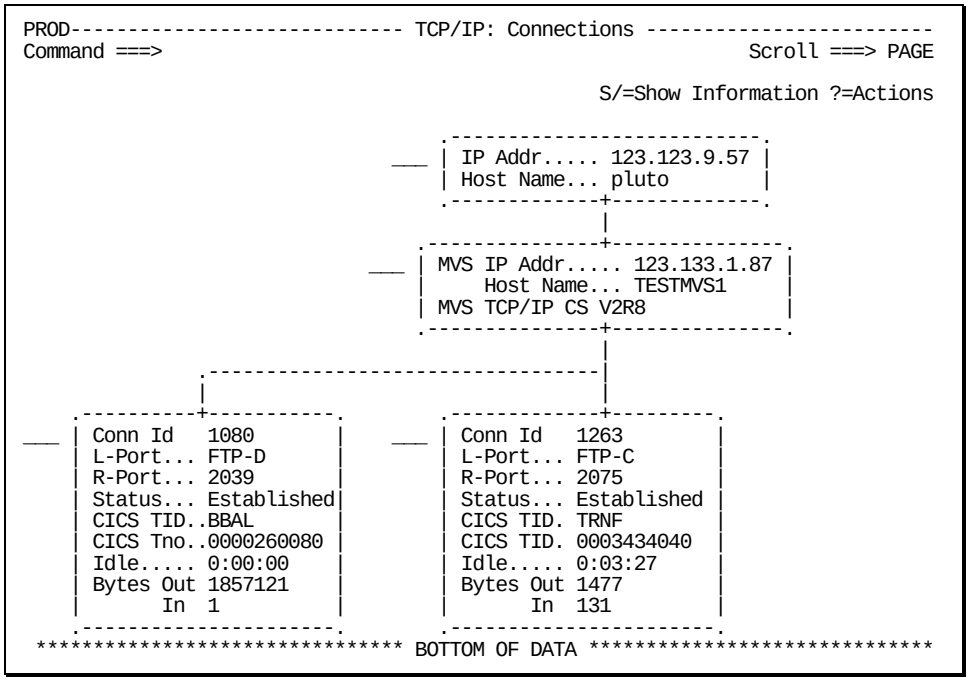
To display the actions that are applicable to each of the layers, enter a question mark (**?**) beside the relevant box on the Telnet Connections Display panel.

For information about the actions available on the Telnet Connections Display panel, press F1 (Help).

Displaying CICS Socket Connections

To present the CICS Socket Connections display for a specific host, enter **S** next to an entry on the CICS Socket Connection List. The Connections panel is displayed.

CICS Socket Connections Display



Fields and Actions on the CICS Socket Connections Display

For details of the information displayed, press F1 (Help).

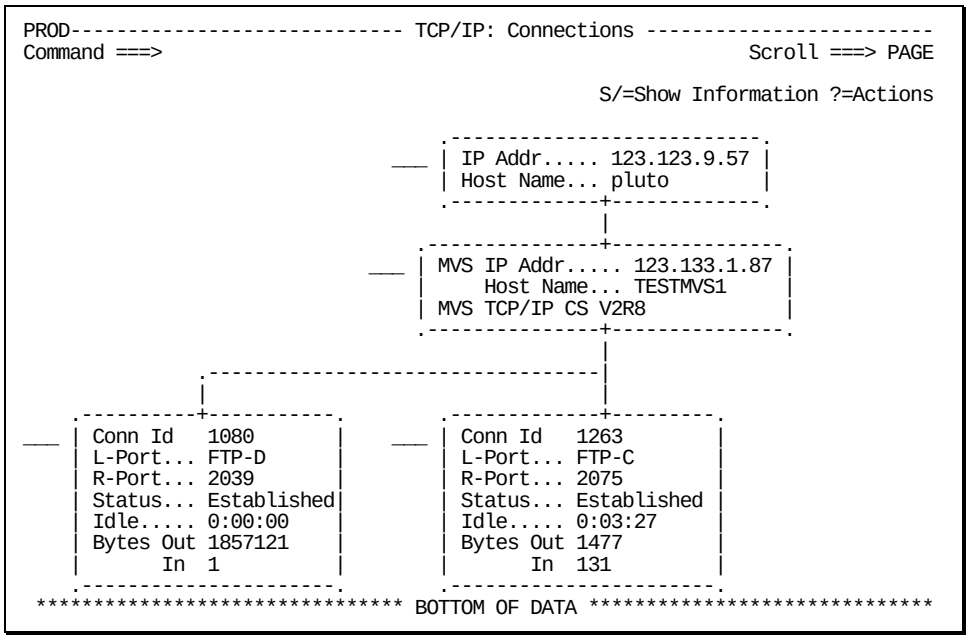
To display the actions that are applicable to each of the layers, enter a question mark (**?**) beside the relevant box on the Connections display panel.

For information about the actions available on the Connections Display panel, press F1 (Help).

Displaying General Connections

To present the Connections display for a specific host, enter **S** next to an entry on the Connection List. The Connections panel is displayed.

Connections Display



Fields and Actions on the Connections Display

For details of the information displayed, press F1 (Help).

To display the actions that are applicable to each of the layers, enter a question mark (**?**) beside the relevant box on the Connections display panel.

For information about the actions available on the Connections Display panel, press F1 (Help).

Displaying Status of TCP/IP Resources

You can use the NETSTAT command from the OCS panel to display the current status of IBM TCP/IP or TCPaccess resources.

For details about the NETSTAT (IBM) command, type NETSTAT on the OCS panel and press F1 (Help).

For details about the NETSTAT (TCPaccess) command, see the *TCPaccess Planning and Operations Guide.*

Listing Specific Connections

You can find a user's connection by entering the user's Telnet LU name or IP address in the Remote Host field on a connection list criteria panel. By specifying either an LU name or IP address, you can restrict a connection list to one particular host.

You can also limit the list by specifying an IP address mask (for example, 172.16.122.*), a Telnet LU name, or an application name mask.

Note: You can specify the mask of an address or name by using the asterisk (*****) and question mark (**?**) wildcards (* matches 0 or more characters, and ? matches exactly one character). For example:

A mask of 172.16.122.* matches 172.16.122.1 and 172.16.122.56.

A mask of 172.16.12?.* matches 172.16.122.1, 172.16.122.56, and 172.16.123.1 but does not match 172.16.12.1 because the ? matches exactly one character.

Finding an LU Name

You can help users find their LU name by asking them to display the primary menu. The user's LU name is displayed at the right side of the screen.

Some other SNA applications also display the connected LU name on a screen within the application. A user can check any individual SNA application to find the LU name.

You can ask users to use the appropriate command for their application to display the LU name for the LU they are using. For example, for a NetMaster application, the SHOW USERS command displays LU names beside user IDs.

Finding an IP Address

Many users call their help desk with a TCP/IP problem and do not know their IP address, particularly if they have implemented the Dynamic Host Configuration Protocol (DHCP) that can cause IP addresses to change from day to day.

You can ask users to find their IP address (for their help desk to specify in the Remote Host field on the TCP/IP : Connections menu) in the following ways:

Using Windows 95 or 98

If you are using Windows 95 or 98 on your PC, you can find your IP address by doing this:

1. From Windows 95 or 98, click Start on the taskbar, and then choose Run.
2. In the Run window, type **WINIPCFG** and click OK.

   The IP configuration window is displayed, showing the current IP address and other information such as adapter address, subnet mask, and the default gateway in use.

Using Windows NT or 2000

If you are using Windows NT or 2000 on your PC, you can find your IP address by doing this:

1. From Windows NT, click Start on the taskbar, and then choose Run.
2. In the Run window, type **CMD** and click OK. A command prompt window is displayed.
3. In the command prompt window, enter the command **IPCONFIG**. The TCP/IP Configuration is displayed, showing the current IP address and other information such as subnet mask and default gateway.

Using PC Application Help

Some PC applications provide an IP address in the Help menu. If you are using a PC application, find your IP address by selecting *Help - About* on your application menu. The displayed window may provide the IP address of your computer.

Chapter 4

Diagnosing Connection Problems

This chapter contains the following topics:

- Testing Connectivity
- Tracing a TCP/IP Route
- Checking for SNA Related Problems on Telnet Connections
- Looking Up a Device Name
- Dropping a Connection
- Diagnosing Data and Protocol Related Problems in a Connection
- Browsing the Local or Remote Activity Logs
- Diagnosing Telnet Response Time Problems
- Diagnosing Throughput of Data Transfers
- Monitoring FTP Workload Performance
- Monitoring Connection Workload Performance

Testing Connectivity

During problem diagnosis, you can use the PING command to do any of the following:

- Test whether a host is reachable through the network
- Determine the host name or IP address of a device
- Determine the network transit time for packets of varying sizes
- Determine whether all packets sent reached their destination

You can use a ping action in several ways:

- Directly check the above information from the TCP/IP : Network Diagnosis Functions menu
- Use the ping action against a host on a list or display
- Issue the PING command from the command line.

Performing a Ping

Performing a ping sends an echo request that tests whether the remote host is reachable through the network and how long a return trip takes.

To test connectivity by sending a ping to a remote host, do the following:

1. Enter **/IPDIAG** at the ===> prompt. The TCP/IP : Network Diagnosis Functions menu is displayed.
2. Type **P** at the ===> prompt on the TCP/IP : Network Diagnosis Functions menu.
3. Type either the name of the remote host or its IP address in the Host Name/Addr field.
4. Press ENTER. The TCP/IP : Ping Result List panel is displayed.

Interpreting Responses to a Ping

The response to a ping is displayed on the TCP/IP : Ping Result List (this is a scrollable list). The following shows an example of the response to a successful ping.

```
PROD---------------------- TCP/IP : Ping Result list ---------------------------
Command ===>                                                  Scroll ===> PAGE

 Target Host Name .... mercury.dept.company.com
        IP Address ... 123.123.2.66
 Count ............... 3__
 Timeout (seconds) ... 5__
 Packet Size ......... 256_
 ------------------------------------------------------------------------------
 Result .............. Successful
 Min/Average/Max Time  10/12/14
 Packets sent ........ 3
         received .... 3
         % lost ...... 0
  Seq No.   Trip Time (ms)
     1      18
     2      14
     3      *
    **END**
```

A ping is an end-to-end transmission between your system and a nominated remote host. When a ping is issued it returns one of the following results:

- Successful
- Packets Lost
- No Response

To determine where on the network, problems such as packet loss, slow response times, or breaks in communication are occurring, you can perform a traceroute. See the section “Tracing a TCP/IP Route” for more information.

If, for example, you are investigating poor end-user response times, packet loss or high trip times might indicate that:

- An unexpected route to the host is being used
- There is congestion on a link or router along the route to the destination host (for example, caused by an unusually large file transfer which might indicate that the particular link or router has insufficient capacity)

Fields on the Ping Result List

For details of the information displayed, press F1 (Help).

Using the PING Line Command

An alternative to using the ping action is to issue the PING line command from either an OCS window or from the Command Entry panel. To obtain the kinds of results returned by the ping action, use the following command form:

PING *ip_address*|*host_name* VERBOSE=YES

See the *Management Services Command Reference* or online help for the syntax of the PING command and a description of each of its operands.

Tracing a TCP/IP Route

It is possible to obtain a *hop-by-hop* record of the route taken by a packet through a network, starting from the source host and finishing at the destination host.

A traceroute can be performed directly from the TCP/IP : Network Diagnosis Functions menu, or it can be done by using the traceroute action against a host on a list or display.

Performing a Traceroute

A traceroute attempts to trace the route from the issuing point through all hosts and routers to the destination host. Otherwise it traces the route to the point at which a break in communication has occurred.

To trace a route to a remote host, do the following:

1. Enter **/IPDIAG** at the ===> prompt. The TCP/IP : Network Diagnosis Functions menu is displayed.
2. Select the **TR** - Trace Route option on the TCP/IP : Network Diagnosis Functions menu.
3. Type either the name of the remote host or its IP address into the Host Name/Addr field and press ENTER. The TCP/IP : Trace Route Result List panel is displayed.

Interpreting Responses to a Traceroute

The Trace Route Result List panel displays the results of the traceroute action (this is a scrollable list). This display is progressively updated as information arrives.

```
PROD------------------- TCP/IP : Trace Route Result List ----------------------
Command ===>                                                  Scroll ===> CSR
 Target Host Name ....  mercury.dept.company.com
        IP Address ...  123.123.2.66
 Result ..............  Unreachable Host
 Hop Limit ...........  10
 Timeout (seconds) ...  3

    P=Ping TN=Telnet S=System Information I=Interfaces R=Routing Table M=Mib-II
                                                 H=History N=IP Node Monitor
    Hop IP Address      Host Name                       Trip Time (ms) Notes
      1 123.0.80.26                                       12   17   15
      2 123.0.80.5                                        50   21   15
      3 123.0.95.4      station4.place.company            19   21   19
      4 123.0.82.1                                        19   19   19
      5 123.123.121.145 sl-gw2-dc-2-7-t1.sprintlink.n     37   24   26
    **END**
```

The most likely reason for performing a traceroute action is that a ping is either unable to reach a remote host or it is indicating slow response times in the TCP/IP network. See the section “Interpreting Responses to a Ping” for more information.

If the ping reported that the host is unreachable, you can do one of the following:

- Perform a traceroute to find out where the failure is occurring
- Check the Routing Table

If the host is unreachable, the traceroute might return a result such as Hop Count Exceeded, Network Unreachable, or Host Unreachable.

If the hop count was exceeded and the IP address column on the last entry or entries is an *, the indication is that a device is not responding (possibly the destination host). If this is the case, or if the result indicated that either the network or host was unreachable, you might want to examine the Routing Table or Interfaces for the last listed hop. You can do this by applying the **I** (Interfaces) or **R** (Routing Table) action against the host or router recorded as the last hop on the list.

When using the Routing Table action, NetMaster for TCP/IP uses masking to ensure that the presented Routing Table contains only those addresses that are relevant to the path you are tracing. This is a network address mask based on the class of address being traced. For example, if you are tracing a route to the foreign host 123.168.2.66, NetMaster for TCP/IP inserts the mask 123.168.2.*.

If the hop count is exceeded and the same number of hops is shown as was set in the Hop Limit field, change the hop limit to a larger number and reissue the traceroute by pressing F6 (Action).

If the ping indicates a slow response, you can check for the following in your traceroute results:

- Check the Notes column to see if there are any outstanding alerts for the node. If the IP Node Monitor is monitoring the node, you can see if any alerts are outstanding.
- Check the trip times—these should increase at a steady rate the further along the route the packets are sent. If there is a sudden and marked increase in the trip time for a particular hop along the route, it might indicate that this is where the problem is occurring. To further investigate:
  - Apply the **I** (Interfaces) action to the host or router at the hop where the problem is occurring and check the Interfaces for clues to the performance degradation
  - Apply the **TN** (Telnet) action to start a Telnet connection to the host or router where the problem is occurring and investigate the configuration or other possible causes
- Check the hop list—if there is no evidence of slow trip times, look at the hop list to check whether an unexpected route is being used.

Note: To analyze response time problems, use the Transaction Path Analyzer facility. See the section “Viewing End-to-end Response Times” for information about this facility.

If the traceroute does not return any abnormal results, use the NetMaster for TCP/IP reporting facility to check for large file transfers.

Fields and Actions on the Trace Route Result List

For details of the information displayed and actions available on the Trace Route Result List, press F1 (Help).

Initiating a Traceroute by Using the TRACEROUTE Line Command

An alternative to using the traceroute action is to issue the TRACEROUTE line command from either an OCS window or from the Command Entry panel. To emulate the kinds of results returned by the traceroute action, use the following command form:

TRACEROUTE *ip_address*

See the *Management Services Command Reference* or online help for the syntax of the TRACEROUTE command and a description of each of its operands.

Checking for SNA Related Problems on Telnet Connections

Problems such as a lost connection or slow response times could be occurring in the SNA rather than the TCP/IP environment. To diagnose SNA problems, you can obtain SNA information about Telnet connections by using Network Control Services (NCS), a facility of NetMaster for SNA that provides full screen displays and navigation of the SNA network.

Note: For IBM TCP/IP stacks, you can also check all Telnet LUs, by applying the CL action to an IBM STACK resource on the IP resource monitor.

Checking the VTAM Status of an LU

Using NCS, you can access detailed status information, configuration, and active session data. To use NCS, do this:

1. Enter **/LISTTEL** at the ===> prompt. The TCP/IP : Telnet Connection List is displayed.
2. To apply the VTAM Display action on the TCP/IP : Telnet Connection List, type **D** beside the appropriate connection on the list and press ENTER. Either the NCS : Resource Display (see the following example) is displayed or a basic VTAM display panel for the selected connection is presented by using an appropriate VTAM display command issued in the Command Entry facility. For information about using NCS, see the *Unicenter NetMaster Network Management for SNA User's Guide.*

```
PROD ---------------------- NCS : Resource Display --------------------------
Command ==>                                                 Scroll ==> CSR

    Information for FTI.SSTCP040        Node Type DYNAMIC APPL
     Status ............... ACT/S       Desired ................ ACTIV
     Major Node ........... SS1APTC1    Type ................... APPL
     Registration Type .... CDSERVR
     Logon Mode Table ..... ISTINCLM
     Default LOGMODE ...... NSX32702
     Session Limit ........ 00000001
     Job Name ............. TCPIP38     Step Name .............. TCPIP38
     Remote IP Address .... 123.35.122.113

    Sessions (1)
          S/=Select Q=Status DS=Display Session D=VTAM Display ?=More Actions
    Name               Status      SID               Send Recv VR TP  ALS
    FTI.STNM1          ACTIV-P     CD2F3C002E17170A  00AF 00DF
    **END**
```

Analyzing SNA Sessions

You can use the **SL** (Session List) action to present the NTS : Session List panel. This panel displays a list of SNA sessions for the LU associated with the selected Telnet connection. You can view a session summary, which includes the following information:

- Activation parameters
- Virtual route status
- Trace and configuration data
- SOLVE:Access MAI session visibility

Because the SNA session list includes historical information, it is possible to view session start and end times, as well as error data.

Note: If your site is not configured with NetMaster for SNA, an appropriate error message is returned when you try to use the Session List action. If your site is configured with NetMaster for SNA but you do not have the display shown in the previous figure, see the *Unicenter NetMaster Network Management for SNA Implementation and Administration Guide* for information on how to set up the Network Tracking System (NTS) of NetMaster for SNA.

To apply the Session List action on the TCP/IP : Telnet Connection List, type **SL** to the left of the appropriate connection on the list and press ENTER. The NTS : Session List for the selected connection is displayed. For information about using NTS, see the *Unicenter NetMaster Network Management for SNA User's Guide.*

```
PROD-------------------------- NTS : Session List ----------------------NET001
COMMAND ===>                                                 SCROLL ===> PAGE

    Sec-Name Pri-Ntwk Pri-Name  Sess-Type   Session-Start   Session-End    Data
    TSTCP007 NET001   TEST1     SDOM LU-LU  27/03 08:57:40  27/03 08:57:51    E
    TSTCP007 NET001   TEST1     SDOM LU-LU  26/03 08:59:59  *** BIND-F ***    E
    TSTCP007 NET001   TEST1     SDOM LU-LU  26/03 02:34:49  26/03 08:59:59    E
    TSTCP007 NET001   TEST1     SDOM LU-LU  25/03 18:06:25  *** BIND-F ***    E
    TSTCP007 NET001   TEST1     SDOM LU-LU  25/03 10:26:27  25/03 18:06:25    E
    TSTCP007 NET001   TEST1     SDOM LU-LU  19/03 09:44:43  19/03 15:30:46    E
    TSTCP007 NET001   TEST1     SDOM LU-LU  20/02 17:14:15  20/02 17:53:50    E
    TSTCP007 NET001   TEST1     SDOM LU-LU  16/08 17:22:05  16/08 17:31:11
    TSTCP007 NET001   TEST4     SDOM LU-LU  09/02 09:47:24  09/02 17:18:02    E
    TSTCP007 NET001   TSTVTM01  SDOM SS-LU  27/03 08:57:40  27/03 08:57:51
    TSTCP007 NET001   TSTVTM01  SDOM SS-LU  26/03 02:34:49  26/03 08:59:59
    TSTCP007 NET001   TSTVTM01  SDOM SS-LU  25/03 10:26:27  25/03 18:06:25
    **END**
```

Looking Up a Device Name

Being able to associate a name with a host, rather than just a series of numbers (the IP address) can make the host easier to identify. For example, the real name of the host might give you information about where that host is actually located—although this depends on the naming standards used by your enterprise.

The **NL** (Lookup) action returns the name of the foreign host.

To look up a device name, type **NL** beside the appropriate connection on the connection list and press ENTER—the response is displayed on the third line of the connection list panel.

Initiating a Lookup Using the NSLOOKUP Line Command

An alternative to using the Lookup action is to issue the NSLOOKUP line command from either an OCS window or the Command Entry panel. To emulate the kinds of results returned by the Lookup action, use the following command form:

NSLOOKUP *ip_address*

Dropping a Connection

Where an error condition exists, for example, the connection seems to have stalled, it might be necessary to drop that connection and have the user reconnect. To drop a connection:

1. Type **Z** beside the appropriate connection on a list or display and press ENTER. You are prompted to confirm your request.
2. Press ENTER to confirm. A message informing you that the connection has been successfully dropped is displayed and the connection is highlighted on the connection list as having been dropped.

```
PROD------------------ TCP/IP : Telnet Connection List ------------------SOLV02
Command ===>                                                  Scroll ===> PAGE
EZA0109I Connection successfully dropped
 Line 1 of 6                                     Refresh Every ... ___  Seconds
  P=Ping T=TraceRoute D=VTAM Display SL=Session List NL=Lookup S/V=View Z=Drop
                MT=Mini Trace TPA=Transaction Path Analyzer L=Log ?=Actions
    Foreign Host    LU       Appl     Status     Bytes Out Bytes In
    123.183.154.85  SDTCP001 TEST1    Establshd     350931    64662
    123.0.128.73    SDTCP003 TEST1    Establshd      19605     3264
    123.0.92.60      ***DROPPED***
    123.0.92.60     SDTCP005 TEST1    Establshd     290756     1240
    123.0.228.251   SDTCP006 TEST1    Establshd     182225    23586
    123.0.128.73    SDTCP008 TEST1    Establshd     160616     4331
    **END**
```

Diagnosing Data and Protocol Related Problems in a Connection

Data moves around the TCP/IP network in the form of IP packets. You use the packet trace facility to diagnose data- and protocol-related problems over the TCP/IP network.

If you are experiencing a problem such as an unexpected disconnection, you can activate IP packet tracing.

This facility can be used only with IBM TCP/IP and TCPaccess. It is not available for Cisco channel cards.

When you use packet tracing on the TCP/IP : Telnet Connection List, the packet trace is always performed on the IP address in the Foreign Host column.

If there is no Foreign Host IP address, the packet trace is performed on the local port number (for example, in the case of UDP or Listen entries).

You might also want to trace the SNA side of a TN3270 connection by using the Network Tracking System (NTS). For information about using NTS, see the *Unicenter NetMaster Network Management for SNA User's Guide.*

Browsing the Local or Remote Activity Logs

The activity log allows you to browse all messages written to the log for any specified link name from one point. The activity log lists activities that have been occurring on your system, including activities relating to Telnet, FTP, and TN3270 connections.

Note: For TCPaccess, NetMaster for TCP/IP can collect messages issued by TCPaccess and display each message in the activity log.

To access the activity log from anywhere within the NetMaster for TCP/IP region, do any of the following:

- Enter /LOG or $LOG at the ===> prompt on a panel to display the activity log for the local region.
- Enter $LOG *linkname* at the ===> prompt on a panel to display the activity log for the specified linked region.
- Press F7 in OCS.

If you want a selection list of link names, you can do the following to access the activity log:

1. Enter **/HISTORY** at a ===> prompt. The Historical Data : Primary Menu is displayed.
2. Type **L** at the ===> prompt on the Historical Data : Primary Menu.
3. Enter **?** in the Link or Domain Name field.
4. Select an option from the displayed domain list.

   Note: If you specify a link in the Link or Domain Name field, the log displays messages from the activity log for the system represented by that link name.

For information about browsing the online activity log, press F1 (Help) from the activity log panel.

To view the activity log, you can also enter **L** (Display Activity Log) next to an entry on any connection list.

Customizing the Activity Log

You can customize your view of the activity log in the following ways:

- Filtering
- Finding text
- Positioning by day and time

You can also print the log.

For further information, press F1 (Help) from the activity log panel.

Telnet Activity in the Log

For IBM TCP/IP users, Telnet connections can be logged as they are started and ended. For TCPaccess users, only end messages can be logged.

Note: Whether or not these messages are logged is set by your system administrator.

Examples of Telnet connection start and end messages are:

IPCM2002 TELNET CONNECTION STARTED FROM 123.168.2.66..4925 AS TSTCP007 TO TEST1 LOGICAL DEVICE 0006

IPCM2003 TELNET CONNECTION ENDED FROM 123.168.6.127 AS TSTCP006 TO TEST4, BYTES IN 550 OUT 32665 DURATION 0 DAYS 00.06.35

From the log, you can obtain the following information:

- The time that the connection started, plus the port number, LU, and device number used
- The time that the connection ended, the IP address and LU name of the device where the connection ended, the application to which the session was connected, the number of bytes in and out, and the duration of the connection

FTP Activity in the Log

From the log, you can obtain information about the following FTP activities associated with FTP server and client processing:

- File transfers

  Provides information including user's IP address, the dataset name and size, and how long the file transfer took.

- Deletion and renaming of files by using the FTP facility

  Provides the name of the file being deleted or renamed, and the new name for a file being renamed.

- Failures

  Provides a record of failed logons and failed transfers.

Note: Whether or not these messages are logged is set by your system administrator.

Examples of FTP messages are:

IPFM2103 FTP RETR BY USER01 AT 123.168.9.57 DSN AUDE0.TEST01.BIGFILE 1872317 BYTES IN 43.56 SECONDS 42982 BYTES / SEC SERVER FTPTEST1

IPFM2102 FTP LOGON FAILED FOR USR02 AT 123.168.7.23 SERVER FTPTEST1

Connection Activity in the Log

IBM TCP/IP and TCPaccess connection start and end can be logged in the activity log.

Note: Whether or not these messages are logged is set by your system administrator.

Examples of connection messages are:

IPCM2311 CONNECTION OPENED: LOCAL ADDR=123.168.1.2..1081 REMOTE ADDR=123.168.8.2..2360 JOBNAME=SRVTSK3

IPCM2312 CONNECTION CLOSED: LOCAL ADDR=123.168.1.2..1081 REMOTE ADDR=123.168.8.2..2360 JOBNAME=SRVTSK3 BYTES IN=310 BYTES OUT=464

Diagnosing Telnet Response Time Problems

By providing an evaluation of the components that make up a user's response time, the Telnet Transaction Path Analyzer allows you to diagnose response time problems. The response time components that it evaluates are:

- IP network
- Telnet server
- SNA network
- Application

To provide this evaluation, the Transaction Path Analyzer:

- Monitors the IP network for the client
- Checks the responsiveness of the Telnet server
- Monitors the SNA session for application and network response time

Viewing End-to-end Response Times

By providing a view of end-to-end response times, the Transaction Path Analyzer supports the diagnosis of network and system performance.

To use the Transaction Path Analyzer:

1. Access a Telnet connection list.
2. At a connection list, type **TPA** next to the session that you want to view.

The Telnet Transaction Path Analysis panel is displayed (see the following example) for the session you selected. The panel displayed for a Telnet connection is different from that displayed for a connection by task name. For information about the latter display, see the section “Diagnosing Throughput of Data Transfers”.

```
PROD------------- TCP/IP : Telnet Transaction Path Analysis ---------Link: PROD
Command ===>

Estimated User Response ......... 5.470s
Number of Hops to Client .. 5
.--------------------.    .--------------------------.    .-----------------.
|  Job SOLV01        +----+  Host TN3270 Server      +----+   Client        |
| PLU ... NM001        RTM  SLU ..... SSTCP030         RTM  192.0.99.111    |
| Netid . NET        0.002s PU Name . N/A            0.440s                 |
| RTM ... 4.984s     +----+ IP Addr . 192.0.88.22    +----+                 |
'--------------------'    | RTM ..... 0.044s         |    '-----------------'
                          '--------------------------'

Key:  A-Application   S-SNA Network   T-Telnet Server   I-IP Network
.---------------------------------------------------------------------------.
| AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAASTII |
'---------------------------------------------------------------------------'
IPSM0105 NET01 --> SSTCP030 APPLICATION SEND, RESPONSE TIME 4.784s, OPERATION W
IPSM0107 NET01 <-- SSTCP030 TERMINAL RESPONSE, NETWORK PATH TIME 0.002s.
IPSM0106 NET01 <-- SSTCP030 TERMINAL INPUT, KEY ENTER, LENGTH 8.
IPSM0105 NET01 --> SSTCP030 APPLICATION SEND, RESPONSE TIME 4.984s, OPERATION W
IPSM0107 NET01 <-- SSTCP030 TERMINAL RESPONSE, NETWORK PATH TIME 0.002s.
```

Fields and Actions on the Transaction Path Analysis Panel

For details of the information displayed and actions available on the Transaction Path Analysis panel, press F1 (Help).

Messages

Messages are displayed on the Transaction Path Analysis panel to show the status of actions performed. An example is:

IPGP1212 PING hubble.dept.company.com(123.0.80.25): TIME=3/3/4 MS

Old messages scroll as new messages are received. To view all messages, press F7 (Log).

Session Awareness Messages

Examples of session awareness messages available after pressing F5 to start monitoring sessions are:

IPSM0107 STNM1 <-- SDTCP042 TERMINAL RESPONSE, NETWORK PATH TIME 0.002s.

IPSM0105 STNM1 --> SDTCP042 APPLICATION SEND, RESPONSE TIME N/A, OPERATION WRIT

IPSM0106 STNM1 <-- SDTCP042 TERMINAL INPUT, KEY PF03, LENGTH 3.

IPSM0105 STNM1 --> SDTCP042 APPLICATION SEND, RESPONSE TIME 0.535s, OPERATION W

Diagnosing Throughput of Data Transfers

By providing an evaluation of the characteristics that make up IP connections, the Transaction Path Analyzer allows you to diagnose any throughput problems of data transfers. (See the following example for listing connections by task name.) The characteristics that it evaluates are:

- The average data transfer rate between the IP server and IP client for the elapsed time from timed samples
- Response time
- Hop length
- Alert indicator

```
PROD----------------- TCP/IP : Transaction Path Analysis ----------------------
Command ===>

Number of Hops to Client .. 4  Number with Alerts .. 1  (Press F8 to View)
.---------------+-------------------------.        .-------------------------.
|    Server     |     OS/390 TCP/IP       +--------+       Client            |
| Task INTCLIEN | IP Addr 123.0.88.22     IP Network  IP Addr 123.0.99.111   |
| Port TELNET   | RTM ... 0.018s          RTM 0.519s  Port .. 1076            |
|               | abcmvs1.weston.abc.comp +--------+                          |
'---------------+-------------------------'        '-------------------------'

IPTP0711 --Time--  Bytes Out  Kb/Sec   Bytes In  Kb/Sec  --Idle--
IPTP0712 09.16.24      70935       -       5941       -   0:00:01
IPTP0712 09.16.43      72783   0.095       5952   0.001   0:00:01
IPTP0701 09.25.34 MONITOR STARTED
```

Viewing End-to-end Throughput

By providing a view of end-to-end throughput times, the Transaction Path Analyzer supports the diagnosis of network and system performance.

1. Access a connection list by task name.
2. At a connection list, type **TPA** next to the session that you want to view.

To use the Transaction Path Analyzer, do this:

1. Access a connection list by task name.
2. At a connection list, type **TPA** next to the session that you want to view.

Note: The TPA action is not allowed on connections that do not have a foreign host, as indicated by the asterisk (*) in the Foreign Host column of any connection list.

The Transaction Path Analysis panel is displayed for the session you selected. The panel displayed for a connection by task name is different from that displayed for a Telnet connection. For information about the latter display, see the section “Diagnosing Telnet Response Time Problems”.

Fields and Actions on the Transaction Path Analysis Panel

For details of the information displayed and actions available on the Transaction Path Analysis panel, press F1 (Help).

Monitoring FTP Workload Performance

The Monitor FTP Workload Performance panel provides information and displays graphs of the performance data for the FTP workload. The FTP workload performance data includes:

- Bytes transferred for a given host
- Bytes transferred by application for this host
- Bytes transferred by network for this host
- Number of transfers for this host
- Number of transfers by application for this host
- Number of transfers by network for this host
- Number of FTP failures for this host
- Number of FTP failures by application for this host
- Number of FTP failures by network for this host

For FTP data to be passed to the FTP workload performance facility, the following fields must be set on the IPMONITOR - TCP/IP Logging and Monitoring panel of the ICS initialization parameters:

- Receive FTP Events? - YES
- Report FTP Events? - YES
- Analyze FTP Workload? - YES

For further information about setting these parameters, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide*.

To display the Monitor FTP Workload Performance panel, enter **WF** (FTP Workload Data) next to a stack name on the IP resource monitor.

For further information about the workload performance display, press F1 (Help) from the display panel.

Monitoring Connection Workload Performance

The Monitor Connection Workload Performance panel provides information and displays graphs of the performance data of the connection workload. Connection workload performance data includes:

- Bytes for all connections to this host
- Bytes for connections by application for this host
- Number of connections for this host
- Number of connections by application for this host
- Number of connections by network for this host

For connection event data to be passed to the performance facility, the following fields must be set on the IPMONITOR - TCP / IP Logging and Monitoring panel of the ICS initialization parameters:

- Receive Connection Events? - YES
- Report Connection Events? - YES
- Analyze Connection Workload? - YES

For further information about setting these parameters, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

To display the Monitor Connection Workload Performance panel, enter **WC** (Connection Workload Data) next to a stack name on the IP resource monitor.

For further information about using the IP resource monitor, see the Managing IP Resources chapter.

For further information about the workload performance displays, press F1 (Help) from each display panel.

Monitoring Telnet Workload Performance

The Monitor Telnet Workload Performance panel allows you to view and graph the Telnet workload of your system. The attributes monitored are the total number of Telnet connections for a foreign host with a connection to this OS/390 or z/OS application.

For connection event data to be passed to the performance monitor, TN3270 fields must be set by your network administrator by using ICS. For further details, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

To display the Monitor Telnet Workload Performance panel, enter WT (Telnet Workload Data) next to a stack entry on the IP Resource Monitor.

For details of the information displayed, press F1 (Help).

Chapter

5

Managing IP Resources

This chapter contains the following topics:

- Managing IP Resources
- Monitoring IP Resources
- IP Resource Classes
- Adding an IP Resource to the IP Resource Monitor

Managing IP Resources

IP resources in or adjacent to your local LPAR can be managed from the IP resource monitor.

The IP resources to be monitored are defined in a system image. When you start up the region, the system image is loaded automatically and the resources in the image are visible on the IP resource monitor.

This chapter provides an overview of how to use NetMaster for TCP/IP to manage your IP resources.

You can use IP resource filters to select which resources are displayed in the list. The IP resource monitor displays the status of the resources selected by the filter identified in the title. If you arrive at the monitor from the primary menu, the title identifies objects being monitored.

In a multisystem environment, resources from all linked regions are, by default, visible on the IP resource monitor in any focal region. You can manage all resources from a central IP resource monitor.

Monitoring IP Resources

You manage your IP resources from the IP resource monitor. To access the IP resource monitor, enter **/IPMON** at the ===> prompt. The Status Monitor : IP Resources panel is displayed. This is the IP resource monitor.

```
PROD------------------- Status Monitor : IP Resources -------------PROD18-0001
Command ===>                                                 Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                          Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual  Status   Count  Sev  Samp  Samp
    DEPT         ASMON    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CIPQA18      CIP      DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CSM          CSM      DEPT18   ACTIVE  Ok       4      2    16:17 17:17
    EE           EE       DEPT18   ACTIVE  Ok       0      0    16:37 16:47
    OSADEX       OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    OSAEX        OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    QAS2         OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    ROTQ18       ROUTER   DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPICSD1     STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPIP38      STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

Note: The format of the IP resource monitor can be tailored to your installation's requirements. Your IP resource monitor may not look the same as the one shown here.

Customizing Display Attributes and Formats

The status monitor displays resources line by line. You can customize the display attributes and the display format if you have the appropriate authority. See the *Automation Services Administrator Guide* for information about the default display attributes and the display formats, and how to customize them.

Filtering IP Resources

The FILTER command allows you to display a subset of IP resources being monitored. Supplied filters allow you to display resources of a specified type. You can also define your own filters to select resources based on various criteria.

For further details, press F1 (Help).

User Profile

You can use the PROFILE command to set your own defaults for the IP resource monitor. You can specify default filter, format, and sort criteria. Each time you enter the IP resource monitor, the values in your profile are applied.

Commands on the IP Resource Monitor

There are many commands that you can use on the IP resource monitor to manage your resources. The commands available vary, depending on the type of resource. To view the commands available for a particular resource, enter **?** beside its name.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to the selected resource come first (displayed in turquoise), followed by other generic commands. To execute a command, enter **S** beside it.

Note: The commands available for each resource type are listed in the chapter for that resource type, as shown in the table in the section “IP Resource Classes”.

In a multisystem environment, you can see resources defined in all linked regions. The system name shown for each resource identifies the region. You can apply commands to remote resources in the same way as to local resources.

IP Resource Classes

IP resources belong to various resource classes:

- ASMON—address spaces
- CICMON—CICS resources
- CIP—Cisco channel cards
- CSM—Communications Storage Manager
- EE—Enterprise Extender
- OSA—Open Systems Adapters
- ROUTER—2216 routers
- STACK—TCP/IP stacks (IBM or TCPaccess)

The following chapters describe how to manage resources of each type.

Adding an IP Resource to the IP Resource Monitor

For information about adding IP resources to the IP resource monitor, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide*.

You can add an IP resource directly from the IP resource monitor by pressing F4 (Add).

Chapter 6

Diagnosing the IBM TCP/IP Environment

This chapter contains the following topics:

- Managing Your IBM IP Stack
- Displaying Device Links
- Monitoring Stack IP Performance
- Monitoring Interface Workload Performance
- Issuing Console Commands
- Browsing and Changing the IBM Configuration Datasets
- Changing the Configuration by Using an Obeyfile Dataset
- Checking Telnet LUs
- Displaying Workload of Multiple TCP/IP Stacks
- Displaying the Workload of Telnet Servers

Managing Your IBM IP Stack

You can use the IP resource monitor to display information about, and change the current state of, the IBM TCP/IP stacks on your LPAR.

TCP/IP stacks are shown as class STACK.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources -------------------------
Command ===>                                                  Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                        Monitor  Alert  Max  Last  Next
    Resource     Class    System  Actual  Status   Count  Sev  Samp  Samp
    DEPT         ASMON    DEPT18  ACTIVE  Ok       0      0    16:17 17:17
    CIPQA18      CIP      DEPT18  ACTIVE  Ok       0      0    16:17 17:17
    CSM          CSM      DEPT18  ACTIVE  Ok       4      2    16:17 17:17
    EE           EE       DEPT18  ACTIVE  Ok       0      0    16:37 16:47
    OSADEX       OSA      DEPT18  ACTIVE  Ok       0      0    16:26 17:26
    OSAEX        OSA      DEPT18  ACTIVE  Ok       0      0    16:26 17:26
    QAS2         OSA      DEPT18  ACTIVE  Ok       0      0    16:26 17:26
    ROTQ18       ROUTER   DEPT18  ACTIVE  Ok       0      0    16:17 17:17
    TCPICSD1     STACK    DEPT18  ACTIVE  Ok       0      0    16:17 17:17
    TCPIP38      STACK    DEPT18  ACTIVE  Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

IP Resource Commands

To view the commands available for an IBM stack, enter **?** next to an IBM stack resource.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to IBM stack resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** next to it.

IBM Stack Commands

The commands specific to IBM stacks are:

Command	Description
AL	View alerts for a resource
AM	Activate monitoring
CL	Check Telnet LUs
CMD	Issue modify to stack
D	Display resource status
DG	Display graphical device links
DL	Display device links
DP	Display profile configuration libraries
H	Show performance history
IC	IP connections
ICA	IP connections for all applications
IM	Inactivate monitoring
IP	View stack IP performance history
IPM	View stack IP performance metrics
LA	List applications with IP connections
O	Execute obeyfile
RT	Display routing table
SWL	Display stack workload
TWL	Display Telnet workload
WC	Connection workload data
WF	FTP workload data
WI	Interface workload data
WT	Telnet workload data

Displaying Device Links

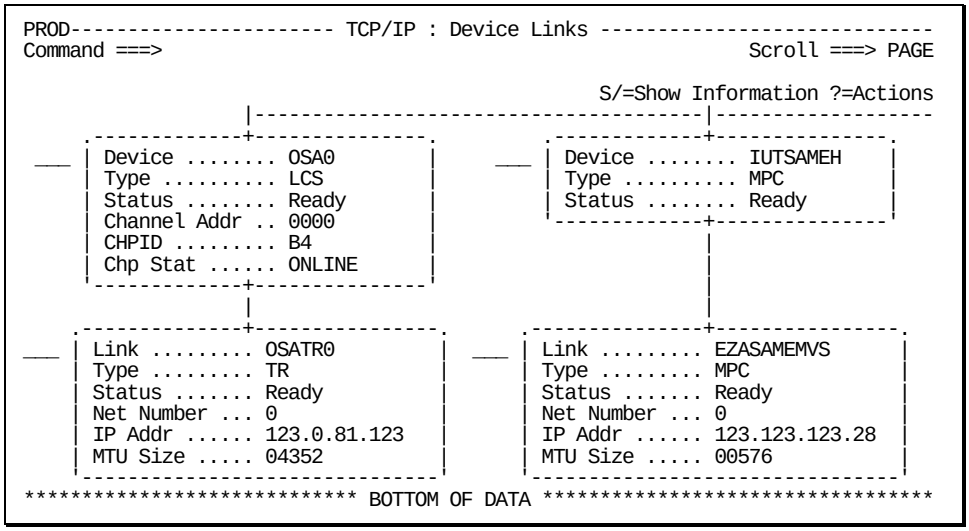
If you are unable to get any connections through the TCP/IP network, or through a particular interface to the TCP/IP network, you might want to check the device links in an attempt to isolate the cause of the problem. To view a list of the TCP/IP interfaces, enter **DL** (Display Device Links) next to an IBM stack on the IP resource monitor. The Device Links List panel is displayed.

```
PROD---------------------- TCP/IP : Device Links List -----------------------
Command ===>                                                 Scroll ===> PAGE

                                                S/=Show Information ?=Actions
     Host Name ......... NMDMVS1
     Description........ MVS TCP/IP CS V2R8

     Device                                                    ----Packets----
     Name                 Type        Status                   In      Out
     LOOPBACK             LOOPBACK    Ready                    497958  501469
     |-- Link Name                                 IP Address      ----Pkts/hr----
         LOOPBACK         LOOPBACK    Ready       123.23.123.132
     OSA0                 LCS         Ready                    -       -
     |-- Link Name                                 IP Address      ----Pkts/hr----
         OSATR0           TR          Ready       123.0.81.123
     VIP0                 VIPA        Ready                    -       -
     |-- Link Name                                 IP Address      ----Pkts/hr----
         SDD1             VIPA        Ready       123.123.123.27
     IUTSAMEH             MPC         Ready                    -       -
     |-- Link Name                                 IP Address      ----Pkts/hr----
         EZASAMEMVS       MPC         Ready       123.123.123.28
     VIPD82C86E13         VIPA        Ready                    -       -
     |-- Link Name                                 IP Address      ----Pkts/hr----
         VIPL82C86E13      VIPA        Ready      130.200.110.19
    **END**
```

For details of the information displayed and actions available, press F1 (Help).

Displaying Device Links Graphically

To view a graphic display of the TCP/IP interfaces, press F4 (GrphDisp). The Device Links panel is displayed. Alternatively, you can enter **DG** beside a stack name on the IP resource monitor (/IPMON).



For details of the information displayed and actions available on the Device Links panel, press F1 (Help).

The Device Links display is organized in three layers:

- The TCP/IP stack
- Devices
- Links

The following describes each of these layers, starting from the top.

The TCP/IP Stack Layer

The first layer represents the TCP/IP software running on this system.

For details of the actions you can apply to the TCP/IP stack layer, press F1 (Help).

Device Layer

The second layer represents the devices used by TCP/IP to interface to the TCP/IP network. Each box in this layer contains the following information for the device:

- Device name
- Channel protocol type (for example, LCS, CLAW, or CTC)
- Device status
- Channel address
- Channel path status (ONLINE or OFFLINE)
- An error message if applicable
- Send queue size

If the error message PATH ERROR or CHP ERROR is displayed for a device, there is an error in the path or the channel path. To investigate this error, use the operating system command: D M=DEV(*devAddress*).

If the error message ERROR STATUS is displayed for a device, there is a configuration error. To investigate this error, see the *IBM TCP/IP for OS/390 Communications Server Installation Guide*.

If the device is running in 3172 offload mode, the word offload is displayed.

SNA link devices display an LU name.

For details of the actions you can apply to a device, press F1 (Help).

Link Layer

The third layer represents the links used by IBM TCP/IP to interface to the TCP/IP network. Each box in this layer contains the following details for each link:

- Name
- Protocol type (for example, ETHERNET or IBMTR)
- IP address of the link
- In Pkts/Hour and Out Pkts/Hour (This information is available only if interface monitoring is set as active on the TCP/IP : Performance Monitor Parameters panel. For more information about setting performance parameters, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide*.)

For details of the actions you can apply to a link, press F1 (Help).

Monitoring Stack IP Performance

The IP resource monitor allows you to monitor two types of IP performance data for a stack:

- Stack performance history
- Stack metrics

Monitoring Stack IP Performance History

To display the Monitor Stack IP Performance History panel, enter **IP** (View Stack IP Performance History) next to a stack entry on the IP resource monitor (/IPMON).

```
PROD------------ TCP/IP : Monitor Stack IP Performance History-----------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... 123.123.123.123
     Description ......... NMDMVS1.XYZ.COM
     Current Alerts ...... 0
                                        E=Expand C=Contract  S/=Summary D=Detail
                                 - Alerts -          Last
   Attribute/Qualifier           Open  Total Samples Sample        Value Type
     |-- ipAddrErrors                     0      14 11:12            0 GAUGE
     |-- ipDelivers                       0      14 11:12         1304 GAUGE
     |-- ipDgrmsForwarded                 0      14 11:12            0 GAUGE
     |-- ipDgrmsUnknwnPro                 0      14 11:12            0 GAUGE
     |-- ipDiscards                       0      14 11:12            0 GAUGE
     |-- ipFragCreates                    0      14 11:12            0 GAUGE
     |-- ipFragFailed                     0      14 11:12            0 GAUGE
     |-- ipFragOk                         0      14 11:12            0 GAUGE
     |-- ipHeaderErrors                   0      14 11:12            0 GAUGE
```

For details of the information displayed and actions available, press F1 (Help).

Monitoring Stack IP Performance Metrics

To display the Monitor Stack IP Performance Metrics panel, enter **IPM** (View Stack IP Performance Metrics) next to a stack entry on the IP resource monitor (/IPMON).

```
PROD-----------------TCP/IP : Stack IP Performance Metrics -Columns 00001 00079
Command ===>                                                  Scroll ===> PAGE

Stack Address ............. 123.123.123.123

******************************** TOP OF DATA ********************************
Stack Name ............................... CS for OS/390 V2R8
Stack Procedure Name ..................... TCPIP38
Date Started ............................. FRI 21-SEP-2001 18:57:16.9
Address Space ID ......................... 83 (decimal)

 TCP Statistics

   Buffer Size - Receive ................. N/A
                 Send ..................... N/A
   Connections - Maximum Supported ....... 32767
                 Currently Established ... 111
                 Resets ................... 0
                 Active Opens ............. 45
                 Passive Opens ............ 0
                 Failures ................. 0
      Segments - Sent ..................... 82806
                 Sent With RST Flag ...... 1693
                 Retransmitted ............ 994
                 Received ................. 84963
                 Received With Errors .... 4025

 UDP Statistics

   Buffer Size - Receive ................. N/A
                 Send ..................... N/A

     Datagrams - In ...................... 11806
                 In With Errors .......... 0
                 In With No Port Avail ... 3
                 Out ..................... 12472

 IP Statistics
                 Routing Support ......... NOT FORWARDING
    Packets In - Total ................... 124176
                 Forwarded ............... 0
                 Delivered ............... 136184
                 Discarded ............... 0
                 Address Errors  ......... 2019
                 Header Errors ........... 0
                 Unknown Protocol ........ 0
   Packets Out - Requested.............. 108660
                 Discarded ............... 0
                 No Routes ............... 0
  Reassemblies - Required ................ 0
                 Packets Reassembled ..... 0
                 Failures ................ 0
                 Reassembly Timeout ...... 7324
Fragmentations - Packets Fragmented ...... 0
                 Failures ................ 0
                 Fragments Created ....... 65535
          Routing Entries Discarded ...... 0
```

For details of the information displayed and actions available, press F1 (Help).

Monitoring Interface Workload Performance

The Monitor Interface Workload Performance panel allows you to analyze and graph the stack's local interface status and packet details. The interface details collected are:

- Inbound packet details
- Outbound packet details
- Interface status

To display the Monitor Interface Workload Performance panel, enter **WI** (Interface Workload Data) next to an IBM stack on the IP resource monitor (/IPMON).

For details of the information displayed and actions available, press F1 (Help).

Issuing Console Commands

You can issue a MODIFY command against the TCP/IP job and see the responses to the command. Both solicited and unsolicited messages from the TCP/IP job are displayed.

To issue console commands, do this:

1. Enter **CMD** (Issue Modify to Stack) next to an IBM stack entry on the IP resource monitor (/IPMON). The Command Entry panel is displayed.

```
PROD------------ Automation Services : Stack Commands ------------Line 1 of 10
Command TCPIP38 ===> D TCPIP,,HELP
                ===>

System PROD        Limit 1000   Wrap OFF   Edit OFF   Scroll OFF   Async ON
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
```

2. Enter a command at the ===> prompt. For example, enter **D TCPIP,,HELP** in this field to issue a help command.

   NetMaster for TCP/IP issues this command as a SYSCMD. The Stack Commands panel displays messages as this command is processed.

```
PROD------------ Automation Services : Stack Commands -------------Line 1 of 5
Command TCPIP38 ===>
                ===>

System PROD        Limit 1000   Wrap OFF   Edit OFF   Scroll OFF   Async ON
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
SYSCMD D TCPIP,TCPIP38,HELP
N86510 COMMAND PASSED TO OPERATING SYSTEM
10:28:09 STC11084   EZZ0371I D...(NETSTAT|TELNET|HELP|DISPLAY|VARY|OMPROUTE|
 EZZ0371I SYSPLEX)
** END OF DELIVERED MESSAGES **
```

For details of the input fields and the actions available, press F1 (Help).

For information about console commands supported by the IBM stack, see the *IBM TCP/IP for OS/390 Communications Server Customization and Administration Guide*.

Browsing and Changing the IBM Configuration Datasets

IBM TCP/IP configuration information is contained in the following datasets:

- PROFILE.TCPIP—the IBM TCP/IP profile
- TCPIP.DATA—the IBM TCP/IP client configuration
- FTP.DATA—the FTP server configuration

For further information about these datasets and how they are used when configuring your system, see the *IBM TCP/IP for OS/390 Communications Server Customization and Administration Guide*.

Browsing and Changing the TCP/IP Configuration

The configuration information required by the IBM TCP/IP application during initialization is defined in the PROFILE.TCPIP dataset. It includes the following kinds of information:

- Telnet server configuration
- Device and link definitions
- Routing information

Browsing the TCP/IP Configuration

To browse the PROFILE.TCPIP dataset:

1. Enter **DP** (Display Profile Configuration Libraries) next to an IBM STACK entry on the IP resource monitor (/IPMON). The Profile Configuration Datasets panel is displayed.

```
PROD------------------- TCP/IP : Profile Configuration Datasets ---------------
Command ===>                                                  Scroll ===> CSR

                                                Use 'S' to select a configuration
     Configuration    Dataset
     Profile TCPIP    TCPIP.DATA.PO(PROFTR)
     TCPIP Data       TCPIP.DATA.PO(DATAD1)
     FTP Data         TCPIP.DATA.PO(FTPDATA)
    **END**
```

2. Enter **S** next to the Profile TCPIP entry. The Browse PROFILE Dataset panel is displayed.

```
PROD------------------- TCP/IP : Browse PROFILE Dataset ----Columns 00001 00079
Command ===>                                                  Scroll ===> CSR

Dataset Name .... TCPIP.DATA.PO(PROFTR)

******************************** TOP OF DATA ********************************
;
; PROFILE.TCPIP   SDD1 Production Stack Main Connection to OSA0.
; =============
;
; ------------------------------------------------------------------------
```

Changing the TCP/IP Configuration

To change the TCP/IP configuration:

1. Press F4 (Edit) from the Browse PROFILE Dataset panel. The Edit PROFILE Dataset panel is displayed.
2. Edit the dataset as required. For information about editing, see the following section, Editing Summary, and the online help for this panel.
3. If you want to cancel the changes you have made on this panel, press F12 (Cancel)—a message is returned on this panel confirming that the changes have been canceled.
4. To save the changes you have made on this panel, do one of the following:
   - Press F4 (Save)—a message is returned on this panel confirming that the changes have been saved.
   - Press F3 (File)—the Browse PROFILE Dataset panel is displayed, with a message confirming that the changes have been saved.

Editing Summary

There are two types of commands that you can use to edit a dataset:

Line Commands—On the left of each line of text is a sequence number field. To update or add text, you can enter commands in these fields to perform edit functions.

Primary Commands—You can enter other commands in the Command ===> field. Commonly used primary commands are assigned to function keys, allowing you to invoke the command by pressing a function key instead of entering the command in the Command ===> field.

For further information about line commands and primary commands, press F1 (Help).

Browsing and Changing the Client Configuration

The configuration information required by the client applications is defined in the TCPIP.DATA dataset. It includes the following kinds of information:

- The host name
- Name server information
- Socket information

Browsing the Client Configuration

To browse the TCPIP.DATA dataset, do this:

1. Enter **DP** (Display Profile Configuration Libraries) next to an IBM STACK entry on the IP resource monitor (/IPMON). The Profile Configuration Datasets panel is displayed.
2. Enter **S** next to a TCPIP Data entry. The Browse TCPIP.DATA Dataset panel is displayed.

```
PROD---------------- TCP/IP : Browse TCPIP.DATA Dataset ----Columns 00001 00079
Command ===>                                                 Scroll ===> CSR

Dataset Name .... TCPIP.DATA.PO(DATAD1)

**** ****************************** TOP OF DATA ******************************
;
;*********************************************************************
;                                                                    *
;   TCPIP38 SDD2 LPAR CTC CONNECTION TO TCPIP31 ON SDD1              *
;                                                                    *
;   COPYRIGHT = NONE.                                                *
;                                                                    *
;   This data, TCPIP.DATA, is used to specify configuration          *
;   information required by TCP/IP client programs.                  *
;                                                                    *
;
```

Changing the Client Configuration

To change the client configuration, perform the following steps:

1. Press F4 (Edit) from the Browse TCPIP.DATA Dataset panel. The Edit TCPIP.DATA Dataset panel is displayed.
2. Edit the dataset as required. For information about editing, see the section "Editing Summary" and the online help for this panel.
3. If you want to cancel the changes you have made on this panel, press F12 (Cancel). A message is returned on this panel confirming that the changes have been canceled.
4. To save the changes you have made on this panel, do one of the following:
   - Press F4 (Save). A message is returned on this panel confirming that the changes have been saved.
   - Press F3 (File). The Browse TCPIP.DATA Dataset panel is displayed, with a message confirming that the changes have been saved.

Browsing and Changing the FTP Server Configuration

For information about the FTP.DATA dataset and how it is used in configuring your system, see the *IBM TCP/IP for OS/390 Communications Server Customization and Administration Guide.*

Browsing the FTP Configuration

To browse the FTP.DATA dataset, do this:

1. Enter **DP** (Display Profile Configuration Libraries) next to an IBM STACK entry on the IP resource monitor (/IPMON). The Profile Configuration Datasets panel is displayed.
2. Enter **S** next to an FTP Data entry. The Browse FTP.DATA Dataset panel is displayed.

```
PROD----------------- TCP/IP : Browse FTP.DATA Dataset ----Columns 00001 00079
Command ===>                                                 Scroll ===> CSR

Dataset Name .... TCPIP.DATA.PO(FTPDATA)

******************************** TOP OF DATA ********************************
;*********************************************************************
;                                                                    *
;   Name of File:            tcpip.SEZAINST(FTCDATA)                 *
;                                                                    *
;   Descriptive Name:         FTP.DATA  (for FTP Client)             *
;                                                                    *
;   SMP/E Distribution Name:  EZAFTCDA                               *
;                                                                    *
;   COPYRIGHT = NONE.                                                *
;                                                                    *
;   This FTP.DATA file is used to specify default file and disk      *
;   parameters used by the FTP client.                               *
```

Changing the FTP Configuration

To change the FTP configuration, perform the following steps:

1. Press F4 (Edit) from the Browse FTP.DATA Dataset panel. The Edit FTP.DATA Dataset panel is displayed.
2. Edit the dataset as required. For information about editing, see the section "Editing Summary" and the online help for this panel.
3. If you want to cancel the changes you have made on this panel, press F12 (Cancel). A message is returned on this panel confirming that the changes have been canceled.
4. To save the changes you have made on this panel, do one of the following:
   - Press F4 (Save). A message is returned on this panel confirming that the changes have been saved.
   - Press F3 (File). The Browse FTP.DATA Dataset panel is displayed, with a message confirming that the changes have been saved.

Browsing the TCP/IP Error Log

The TCP/IP error log is a record of errors that have occurred in the PROFILE.TCPIP dataset and in Obeyfiles. If you run an Obeyfile, which encounters certain errors, NetMaster for TCP/IP refers you to the PROFILE.TCPERROR dataset for information.

To browse the PROFILE.TCPERROR dataset, enter **ERL** (Browse TCP/IP Error Log) next to an IBM STACK entry on the IP resource monitor (/IPMON). The Browse PROFILE.TCPERROR Dataset panel is displayed.

```
PROD------------ TCP/IP : Browse PROFILE.TCPERROR Dataset Columns 00001 00079
Command ===>                                                  Scroll ===> CSR
Dataset Name .... TCPIP.PROFILE.TCPERROR
****************************** TOP OF DATA ********************************
EZB7795E Error encountered in reading TCPIP.DATA.PO(OBEY2):
EZB7843E Line 6:  Subnet masks changed due to mismatches in BSDROUTINGPARMS com
EZB7883I Options enabled after reading TCPIP.DATA.PO(OBEY2):
EZB7762I BSD info for links:
EZB7763I IUCVLNK: BrdAddr 123.11.215.7, DstAddr 123.11.215.6, MaxMtu 2000, Metr
EZB7763I IUCVLNK2: BrdAddr 123.11.215.7, DstAddr 123.0.91.45, MaxMtu 2000, Metr
EZB7763I OSATR0: BrdAddr 123.0.80.27, DstAddr *, MaxMtu 4352, Metric 0, SubnetM
EZB7763I OSAET1: BrdAddr 123.0.81.255, DstAddr *, MaxMtu 1500, Metric 0, Subnet
***************************** BOTTOM OF DATA ******************************
```

Changing the Configuration by Using an Obeyfile Dataset

To make changes to the configuration, you use an Obeyfile dataset. Changes made using an Obeyfile dataset are dynamic and only affect the running system—they are lost when the IBM TCP/IP system is stopped and restarted.

You might use an Obeyfile dataset to control tracing, start or stop devices, or to add new or temporarily authorized users without having to stop and restart the system.

To execute an Obeyfile dataset, do the following:

1. Enter **O** (Execute Obeyfile) next to an IBM STACK entry on the IP resource monitor (/IPMON). The Command Input Fields panel is displayed.

```
PROD------------------- TCP/IP : STACK Execute Obeyfile ----------------------
Command ===>                                                  Function=Update

. Execute Obeyfile Command Input Field ---------------------------------------.
|                                                                              |
|  Obeyfile Dataset ... ____________________________________ (Required)       |
|                                                                              |
 ------------------------------------------------------------------------------
```

2. Type the name of the dataset in the Obeyfile Dataset field and press F6 (Action).

   You can enter the name of the dataset in either of the following ways:

   - Enter the name of a partitioned dataset (PDS), with no member name. The Obeyfile PDS List is displayed.
   - Enter one of the following:
     - The name of a PDS, with a member name included
     - The name of a sequential dataset

```
PROD---------------------- TCP/IP : Obeyfile PDS List ------------------------
Command ===>                                                Scroll ===> PAGE

                                                  O=Obeyfile E=Edit D=Delete
    Member    VV.MM Created     Changed            Size  Init   Mod    ID
    PKTRACE   01.03 11-APR-2001 11-APR-2001 14:51     3     2     0 USER01
    PKTRACEC  01.00 11-APR-2001 11-APR-2001 14:00     2     2     0 USER01
    TRACEOFF  01.00 10-APR-2001 11-APR-2001 10:19     0     0     0 USER01
    TRACEON   01.01 10-APR-2001 11-APR-2001 10:28     3     0     0 USER01
```

3. If you are displaying the Obeyfile PDS List, select (**O**) the Obeyfile member that you want to execute, and press ENTER. The Obeyfile Confirm panel is displayed.

```
PROD---------------------- TCP/IP : Obeyfile Confirm    ----------------------
Command ===>                                                Scroll ===> PAGE

******************************** TOP OF DATA ********************************
NOTRACE TELNET
SCREEN
****************************** BOTTOM OF DATA ******************************
```

4. If you need to change the dataset, press F4 (Edit). The Edit Obeyfile panel is displayed. For further information, see the section “Editing an Obeyfile Dataset”.
5. On the Obeyfile Confirm panel, press F6 (Action) to accept the contents of the dataset and execute the Obeyfile. You are returned to the menu and a message is displayed indicating that processing is complete.

Checking Your Obeyfile Results

The contents and results of the Obeyfile are recorded in the activity log, which you can access by entering /LOG at the ===> prompt.

If you encounter errors when running an Obeyfile, you might be referred to the PROFILE.TCPERROR dataset. For more information about this dataset, see the section “Browsing the TCP/IP Error Log”.

For information about creating Obeyfile datasets or modifying configuration datasets to change your system’s configuration, see IBM’s *TCP/IP for OS/390 Communications Server Customization and Administration Guide*.

Note: Obeyfiles for starting and stopping packet traces and devices are automatically generated by selecting appropriate options on connection and device link displays. For this reason it is not necessary for you to create obeyfiles for these purposes.

Other Actions on the TCP/IP Obeyfile PDS List Panel

The following actions are available on the Obeyfile PDS List panel:

O (Obeyfile)—The Obeyfile action takes you to the Obeyfile Confirm panel, from where you can use F4 (Edit) to edit the selected member of the dataset. For further information, see the section “Editing an Obeyfile Dataset”.

D (Delete)—The Delete action deletes the selected member of the dataset.

E (Edit)—The Edit action displays the Edit Obeyfile panel. For further information, see the section “Editing an Obeyfile Dataset”.

Editing an Obeyfile Dataset

You can create a new member of an Obeyfile dataset, or you can edit an existing one.

Creating a New Member of an Obeyfile Dataset

To create a new member of an Obeyfile dataset, perform the following steps:

1. On the Obeyfile PDS List panel, enter **E *membername*** or **EDIT *membername*** at the ===> prompt. The Edit Obeyfile panel is displayed.
2. Edit the Obeyfile, using the method described in the following section.

Editing an Existing Member of an Obeyfile Dataset

To edit an Obeyfile dataset member, perform the following steps:

1. Press F4 (Edit) from the Obeyfile Confirm panel. The Edit Obeyfile panel is displayed.

   Note: If you are at the Obeyfile PDS List panel, you can edit an Obeyfile member by entering **E** (Edit) next to a dataset name to display the Edit Obeyfile panel.
2. Edit the dataset as required. For information about editing, see the section "Editing Summary" and the online help for this panel.
3. If you want to cancel the changes you have made on this panel, press F12 (Cancel)—a message is returned on this panel confirming that the changes have been cancelled.
4. To save the changes you have made on this panel, press F4 (Save)—a message is returned on this panel confirming that the changes have been saved.

Note: Obeyfile processing can be used to start and stop traces and to alter the state of the interface devices as well as altering some configuration parameters. The OBEYFILE command is used to execute the IBM TCP/IP configuration commands. For more information about this command, see the *Management Services Command Reference* manual.

Checking Telnet LUs

When the IBM TCP/IP system attempts to use an LU for a Telnet connection request and it encounters an error acquiring the LU, it flags the LU as inactive to the IBM TCP/IP system. This is so that IBM TCP/IP does not try to use the LU for future connections.

Over a period of time, a number of LUs may be flagged as inactive. This reduces the number of possible Telnet sessions available. The Problem Telnet LUs panel allows you to activate the LUs from two perspectives:

- IBM TCP/IP (so they are no longer flagged as inactive)
- VTAM

Note: Checking Telnet LUs may cause a large number of messages to be written to the console and may take some time to complete.

To view Telnet LU information, enter **CL** (Check Telnet LUs) next to an IBM stack entry on the IP resource monitor (/IPMON). The Problem Telnet LUs panel is displayed.

```
PROD---------------------- TCP/IP : Problem Telnet LUs -----------------------
Command ===>                                                  Scroll ===> CSR

    In Use ... 20%  Total LUs ... 30    #In Use ... 6  #Bad LUs ... 2
    Bad Logical Unit 1 of 2                      Refresh Every ... ___ Minutes
          AT=ActTCPIP  IT=InactTCPIP  AV=ActVTAM  IV=InactVTAM  D=VTAMDisplay
    LU Name   TCP/IP State  VTAM State
    SDTCP027  INACTIVE      NEVAC
    SDTCP030  INACTIVE      CONCT
```

For details of the information displayed and actions available, press F1 (Help).

If there are no problem Telnet LUs, then the following message is displayed on the Problem Telnet LUs panel:

IPCK7704 NO TELNET LU PROBLEMS FOUND.

Displaying Workload of Multiple TCP/IP Stacks

The TCP/IP Stack Workload Status panel provides information about registered TCP/IP stacks in a Sysplex and their relative availability. This information allows you to diagnose problems with the Domain Name Server based on the Workload Manager (WLM) on OS/390.

When Communications Server is running in a Sysplex, it can register TCP/IP stacks with the Workload Manager (WLM) on OS/390.

This ability allows information to be obtained about what TCP/IP stacks are registered and their relative availability within the Sysplex. (The Sysplex is defined as a name domain.)

By checking with the WLM about the relative availability of Communications Server and its servers on each OS/390 image, a Domain Name Server (DNS) running within the Sysplex can use this information to route work around the Sysplex.

To access the TCP/IP Stack Workload Status panel, enter **SWL** (Display Stack Workload) next to an IBM stack entry on the IP resource monitor (/IPMON).

```
PROD---------------------- TCP/IP : TCP/IP Stack Workload Status---------------
Command ===>                                                 Scroll ===> PAGE

    Host             IP Address          Weight
    ABCMVS1          123.166.11.22       64
    **END**
```

For details of the information displayed, press F1 (Help).

Displaying the Workload of Telnet Servers

The Telnet Server Status display and the Telnet Cluster List provide the following information:

- Cluster names under which the server is registered
- Port number
- Registration status of Telnet servers running on the local OS/390 image

This information allows you to determine which Telnet server within a Sysplex supports which type of client connection and the relative availability of Telnet server and TCP/IP stack for a particular cluster.

When Communications Server is running in a Sysplex, it can register Telnet servers with the Workload Manager (WLM) on OS/390. Each Telnet server can register under more than one cluster name.

This ability allows information to be obtained about what Telnet servers are registered and their relative availability within the Sysplex. (The Sysplex is defined as a name domain.)

By checking with the WLM about the relative availability of Communications Server and its servers on each OS/390 image, a Domain Name Server (DNS) running within the Sysplex can use this information to direct the client connection to the most appropriate server.

To access the Telnet Server Status, enter **TWL** (Display Telnet Workload) next to an IBM stack entry on the IP resource monitor (/IPMON). The Telnet Server Status panel is displayed.

```
PROD-------------------- TCP/IP : Telnet Server Status -----------------------
Command ===>                                                 Scroll ===> PAGE

                                                                     S=Select
    Cluster Name      Port     Status
    TN3270G           23       Registered
    TN3270F           23       Registered
    TN3270E           23       Registered
    **END**
```

For details of the information displayed, press F1 (Help).

To display the Telnet Cluster List, listing the hosts that support the cluster, enter **S** next to the selected Telnet cluster name on the Telnet Server Status display. The Telnet Cluster List is displayed.

```
PROD------------------- TCP/IP : Telnet Cluster List -------------------------
Command ===>                                                 Scroll ===> PAGE

    Host           IP Address         Telnet   Stack
                                      Weight   Weight
    ABCMVS1        123.168.10.22      64       64
    **END**
```

For details of the information displayed, press F1 (Help).

Chapter 7

Diagnosing the TCPaccess Environment

This chapter contains the following topics:

- Managing Your TCPaccess IP Stack
- Displaying Device Links
- Monitoring Stack IP Performance
- Monitoring Interface Workload Performance
- Issuing Console Commands
- Browsing and Changing the Parameters Library

Managing Your TCPaccess IP Stack

You can use the IP resource monitor to display information about and change the current state of the TCPaccess stacks on the local LPAR.

TCP/IP stacks are shown as class STACK.

To access the IP resource monitor, enter **/IPMON** at a ===> prompt.

```
PROD------------------- Status Monitor : IP Resources -------------------------
Command ===>                                                  Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                          Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual  Status   Count  Sev  Samp  Samp
    DEPT         ASMON    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CIPQA18      CIP      DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CSM          CSM      DEPT18   ACTIVE  Ok       4      2    16:17 17:17
    EE           EE       DEPT18   ACTIVE  Ok       0      0    16:37 16:47
    OSADEX       OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    OSAEX        OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    QAS2         OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    ROTQ18       ROUTER   DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPICSD1     STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPIP38      STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

IP Resource Commands

To view the TCPaccess stack commands available, enter **?** beside a TCPaccess stack resource.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to TCPaccess stack resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** beside it.

TCPaccess Stack Commands

The commands specific to TCPaccess stacks are:

Command	Description
AL	View alerts for a resource
AM	Activate monitoring
CMD	Issue modify to stack
D	Display resource status
DG	Display graphical device links
DL	Display device links
DP	Display parms library (TCPACCESS.PARMS)
H	Show performance history
IC	IP connections
ICA	IP connections for all applications
IM	Inactivate monitoring
IP	View stack IP performance history
IPM	View stack IP performance metrics
LA	List applications with IP connections
RT	Display routing table
UM	Update resource monitoring definition
WC	Connection workload data
WF	FTP workload data
WI	Interface workload data
WT	Telnet workload data

Displaying Device Links

If you are unable to get any connections through the TCP/IP network, or through a particular interface to the TCP/IP network, you might want to check the device links in an attempt to isolate the cause of the problem. To view a list of the TCP/IP interfaces, enter **DL** (Display Device Links) next to a TCPaccess stack on the IP resource monitor. The Device Links List panel is displayed.

```
PROD---------------------- TCP/IP : Device Links List -----------------------
Command ===>                                                Scroll ===> PAGE

                                                S/=Show Information ?=Actions
     Host Name ......... 123.123.110.132
     Description........

     Device                                                      ----Packets----
     Name                Type        Status                      In      Out
     CLAW0308            CLAW        Up                          497958  501469
     |-- Link Name                                IP Address      ----Pkts/hr---
         CLAW0308                     Up         123.123.0.132   -       -
     ET3172              Ethernet    Up                          0       0
     |-- Link Name                                IP Address      ----Pkts/hr---
         ETH10002                     Shutting/1 123.0.81.25     -       -
```

For details of the information displayed and actions available, press F1 (Help).

Displaying Device Links Graphically

To view a graphic display of the TCP/IP interfaces, press **F4** (GrphDisp). The Device Links panel is displayed. Alternatively, you can enter **DG** beside a stack name on the IP resource monitor (/IPMON).

```
PROD---------------------- TCP/IP : Device Links ----------------------------
Command ===>                                                Scroll ===> CSR

                                                S/=Show Information ?=Actions
                                        .-------------------------------.
                                    ___ | ABCMVSACST.ABC.COMPANY.COM.  |
                                        '---------------+---------------'
                    .-----------------------------------+
    .---------------+---------------.       .---------------+---------------.
    | Device ........ CLAW0306      |   ___ | Device ........ ET3172        |
    | Type .......... CLAW          |       | Type .......... Ethernet      |
    | Status ........ Up            |       | Status ........ Up            |
    | Channel Addr .. 0306          |       | Channel Addr .. 0002          |
    | Chp Stat ...... UNKNOWN       |       | Chp Stat ...... UNKNOWN       |
    | MAC Address ... 000000000000  |       | MAC Address ... 0020350472A5  |
    | Packets In .... 6568          |       | Packets In .... 44362         |
    | Packets Out ... 8233          |       | Packets Out ... 8             |
    '---------------+---------------'       '---------------+---------------'
                    |                                       |
    .---------------+---------------.       .---------------+---------------.
    | Link ......... CLAW0306       |   ___ | Link ......... ETH10002       |
    | Status ....... Up             |       | Status ....... Up             |
    | IP Addr ...... 123.168.10.21  |       | IP Addr ...... 123.0.81.25    |
    | SubNet Addr .. 123.168.10.16  |       | SubNet Addr .. 123.0.81.24    |
    | SubNet Mask .. 123.255.255.240|       | SubNet Mask .. 123.255.255.252|
    | MTU Size ..... 4096           |       | MTU Size ..... 1500           |
    | In Pkts/Hour . 57             |       | In Pkts/Hour . 1763           |
    | Out Pkts/Hour  153            |       | Out Pkts/Hour  0              |
```

For details of the information displayed and actions available, press F1 (Help).

To return to the Device Links List panel, press F4 (ListDisp).

The TCP/IP : Device Links display is organized in three layers:

- The TCP/IP stack
- Devices
- Links

The following describes each of these layers, starting from the top.

The TCP/IP Stack

The first layer represents the TCP/IP software running on this system.

For details of the actions you can apply to the TCP/IP stack layer, press F1 (Help).

Devices

The second layer represents the devices used by TCP/IP to interface to the TCP/IP network. Each box in this layer contains the following information for the device:

- Device name
- Channel protocol type (for example, LCS, CLAW, or CTC)
- Device status
- Channel address
- Channel path status (ONLINE or OFFLINE)
- An error message if applicable
- Send queue size
- MAC address of the device
- Number of packets received
- Number of packets sent

If the error message PATH ERROR or CHP ERROR is displayed for a device, there is an error in the path or the channel path. To investigate this error, use the operating system command: D M=DEV(*devAddress*).

If the error message ERROR STATUS is displayed for a device, there is a configuration error. To investigate this error, see the *TCPaccess Installation Guide*.

If the device is running in 3172 offload mode, the word offload is displayed.

SNA link devices display an LU name.

For details of the actions you can apply to a device, press F1 (Help).

Links

The third layer represents the links used by TCPaccess to interface to the TCP/IP network. Each box in this layer contains the following details for each link:

- Link name
- IP address
- Network address
- Network mask
- SubNet address
- SubNet mask
- MTU size

For details of the actions you can apply to a link, press F1 (Help).

Monitoring Stack IP Performance

The IP resource monitor allows you to monitor two types of IP performance data for a stack:

- Stack performance history
- Stack metrics

Monitoring Stack IP Performance History

To display the Monitor Stack IP Performance History panel, enter **IP** (View Stack IP Performance History) next to a stack entry on the IP resource monitor (/IPMON).

```
PROD------------ TCP/IP : Monitor Stack IP Performance History-----------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... 123.123.123.123
     Description ......... stack07.abc.com
     Current Alerts ...... 0
                                        E=Expand C=Contract  S/=Summary D=Detail
                                - Alerts -          Last
   Attribute/Qualifier          Open  Total Samples Sample        Value Type
     |-- ipAddrErrors                    0      14 11:12            0 GAUGE
     |-- ipDelivers                      0      14 11:12         1304 GAUGE
     |-- ipDgrmsForwarded                0      14 11:12            0 GAUGE
     |-- ipDgrmsUnknwnPro                0      14 11:12            0 GAUGE
     |-- ipDiscards                      0      14 11:12            0 GAUGE
     |-- ipFragCreates                   0      14 11:12            0 GAUGE
     |-- ipFragFailed                    0      14 11:12            0 GAUGE
     |-- ipFragOk                        0      14 11:12            0 GAUGE
     |-- ipHeaderErrors                  0      14 11:12            0 GAUGE
```

For details of the information displayed and actions available, press F1 (Help).

Monitoring Stack IP Performance Metrics

To display the Monitor Stack IP Performance Metrics panel, enter **IPM** (View Stack IP Performance Metrics) next to a stack entry on the IP resource monitor (/IPMON).

```
PROD-----------------TCP/IP : Stack IP Performance Metrics -Columns 00001 00079
Command ===>                                                  Scroll ===> PAGE

Stack Address ............. 123.123.123.123

******************************** TOP OF DATA *********************************
Stack Name ............................... (not available)

 TCP Statistics

   Connections - Maximum Supported ....... 32767
                 Currently Established ... 111
                 Resets .................. 0
                 Active Opens ............ 45
                 Passive Opens ........... 0
                 Failures ................ 0
      Segments - Sent ..................... 82806
                 Sent With RST Flag ...... 1693
                 Retransmitted ........... 994
                 Received ................ 84963
                 Received With Errors .... 4025

 UDP Statistics

     Datagrams - In ...................... 11806
                 In With Errors .......... 0
                 In With No Port Avail ... 3
                 Out ..................... 12472

 IP Statistics
                 Routing Support ......... NOT FORWARDING
    Packets In - Total ................... 124176
                 Forwarded ............... 0
                 Delivered ............... 136184
                 Discarded ............... 0
                 Address Errors  ......... 2019
                 Header Errors ........... 0
                 Unknown Protocol ........ 0
   Packets Out - Requested.............. 108660
                 Discarded ............... 0
                 No Routes ............... 0
  Reassemblies - Required ................ 0
                 Packets Reassembled ..... 0
                 Failures ................ 0
                 Reassembly Timeout ...... 7324
Fragmentations - Packets Fragmented ...... 0
                 Failures ................ 0
                 Fragments Created ....... 65535
```

For details of the information displayed and actions available, press F1 (Help).

Monitoring Interface Workload Performance

The Monitor Interface Workload Performance panel allows you to analyze and graph the stack's local interface status and packet details. The interface details collected are:

- Inbound packet details
- Outbound packet details
- Interface status

To display the Monitor Interface Workload Performance panel, enter **WI** (Interface Workload Data) next to a TCPaccess stack on the IP resource monitor (/IPMON).

For details of the information displayed and actions available, press F1 (Help).

Issuing Console Commands

The Automation Services : Stack Commands panel allows you to issue modify commands against the TCP/IP job and to see the responses to the command. Both solicited and unsolicited messages from the TCP/IP job are displayed.

To issue console commands:

1. Enter **CMD** (Issue Modify to Stack) next to a STACK entry on the IP resource monitor (/IPMON). The Command Entry panel is displayed.

```
PROD------------ Automation Services : Stack Commands ------------Line 1 of 10
Modify   TCPICSD1 ===> HELP
                  ===>

System PROD        Limit 1000   Wrap OFF   Edit OFF   Scroll OFF   Async ON
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
```

2. Enter a command at the ===> prompt. For example, enter **HELP** in this field to issue a help command. NetMaster for TCP/IP issues this command as a modify command.

   The Stack Commands panel displays messages as this command is processed.

```
PROD------------ Automation Services : Stack Commands -----------Line 1 of 10
Modify   TCPICSD1 ===>
                  ===>

Jobname TCPIP31    Limit 1000   Wrap OFF   Edit OFF   Scroll OFF   Async ON
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
SYSCMD F TCPICSD1,HELP
N86510 COMMAND PASSED TO OPERATING SYSTEM
T00IJ000I HELP
T00IJ090I Help for cmnd: HELP
 Syntax:
        HELP < cmnd-name | COMMANDS | GENERAL >
 Function:
        Display Help information about operator commands.
 Operands:
        cmnd-name: The command for which help is requested.
        COMMANDS: Display available commands.
        GENERAL: General IFS command format information.
Help command complete
** END OF DELIVERED MESSAGES **
```

For details of the input fields and the actions available, press F1 (Help).

For information about console commands supported by TCPaccess, see the *TCPaccess Planning and Operations Guide.*

Browsing and Changing the Parameters Library

The TCPaccess parameters library contains all the configuration file members that provide parameters for the various task groups within TCPaccess.

To browse the TCPACCESS.PARMS dataset, do the following:

1. Enter **DP** (Display Parms Library (TCPACCESS.PARMS)) beside a TCPaccess STACK entry on the IP resource monitor (/IPMON). The TCP/IP : Command Input Fields panel is displayed.

```
PROD--------------------- TCP/IP : Stack Browse Parms -------------------------
Command ===>                                                 Function=Update

 .- Browse TCPACCESS.PARMS Command Input Field ------------------------------.
 |                                                                           |
 |  Dataset Name ... _____________________________________________  (Required)  |
 |                                                                           |
 |  Member Name .... ________                                       (Optional)  |
 |                                                                           |
  ---------------------------------------------------------------------------
```

2. Type the name of your TCPaccess Parameters Library dataset in the Dataset field and press F6 (Action). The TCPaccess Parameters Library List panel is displayed.

```
PROD------------ TCP/IP : TCPaccess Parameters Library List -------------------
Command ===>                                                 Scroll ===> PAGE

                                                  S/B=Browse E=Edit D=Delete
     Dataset Name ... TCPICS.V5R3.PARM

    Member    VV.MM Created     Changed           Size  Init   Mod   ID
    APPCFGD2  01.12 27-JUL-1998 26-OCT-1998 10:31   261   258     0 USER01
    APPCFG00  01.00 28-JUN-1999 28-JUN-1999 17:38     0     0     0 USER01
    APPLUP00  01.01 29-JUN-1999 29-JUN-1999 14:59     0     0     0 USER01
    DNRALCD1  01.03 20-JUL-2000 15-AUG-2001 12:32     7     6     0 USER01
    DNRALCD2  01.14 27-JUL-1998 16-AUG-2001 11:10    14     6     0 USER01
    DNRALC00  01.01 28-JUN-1999 19-DEC-2000 10:39     6     0     0 USER01
    DNRCFGD1  01.03 20-JUL-2000 21-JUL-2000 11:03    31    31     0 USER01
    DNRCFGD2  01.13 27-JUL-1998 15-AUG-2001 14:14    30    29     0 USER01
    DNRCFG00  01.00 28-JUN-1999 28-JUN-1999 17:38     0     0     0 USER01
    DNRHSTD1  01.13 21-JUL-2000 15-AUG-2001 15:32    32    23     0 USER01
    DNRHSTD2  01.23 27-JUL-1998 15-AUG-2001 15:34    47    27     0 USER01
```

For details of the information displayed and actions available, press F1 (Help).

Browsing and Changing a PARMS Member

You can select members from the TCPaccess parameters library list to browse their configuration. You can also change the configuration, if necessary, by editing these members.

Browsing a PARMS Member

To browse a TCPaccess PARMS member, enter **S** or **B** (Browse) beside it on the TCPaccess Parameters Library List panel. The Browse TCPaccess PARMS Dataset panel is displayed.

```
PROD--------------- TCP/IP : Browse TCPaccess PARMS Dataset ----Columns 001 079
Command ===>                                                 Scroll ===> PAGE

Dataset Name .... TCPICS.V5R3.PARM(DNRNSC00)

******************************** TOP OF DATA ********************************
OUR.COM.  SERVERA.OUR.COM. XXX.XX.XX.X  <== SET SERVER FOR YOUR DOMAIN
OUR.COM.  SERVERB.OUR.COM. XXX.XX.XX.X  <== SET SERVER FOR YOUR DOMAIN
IN-ADDR.ARPA. SERVERC.OUR.COM. XXX.XX.XX.X <== SET SERVER FOR DOMAIN
.         NS.INTERNIC.NET.   198.41.0.4     ROOT NAME SERVER
.         KAVA.NISC.SRI.COM. 192.33.33.24   ROOT NAME SERVER
.         C.NYSER.NET.       192.33.4.12    ROOT NAME SERVER
.         TERP.UMD.EDU.      128.8.10.90    ROOT NAME SERVER
.         NS.NASA.GOV.       128.102.16.10  ROOT NAME SERVER
.         NS.NIC.DDN.MIL.    192.112.36.4   ROOT NAME SERVER
.         AOS.BRL.MIL.       128.63.4.82    ROOT NAME SERVER
.         NIC.NORDU.NET.     192.36.148.17  ROOT NAME SERVER
****************************** BOTTOM OF DATA ******************************
```

Changing a PARMS Member

To change a PARMS member, perform the following steps:

1. Press F4 (Edit) from the Browse TCPaccess PARMS Dataset panel. The Edit TCPaccess PARMS Dataset panel is displayed.

   Note: If you are at the TCPaccess Parameters Library List panel, you can edit a member by entering **E** (Edit) beside a member name to display the Edit TCPaccess PARMS Dataset panel.

2. Edit the member as required.
3. If you want to cancel the changes you have made on this panel, press F12 (Cancel)—a message is returned on this panel confirming that the changes have been cancelled.
4. To save the changes you have made on this panel, do one of the following:
   - Press F4 (Save)—a message is returned on this panel confirming that the changes have been saved.
   - Press F3 (File)—the Browse TCPaccess PARMS Dataset panel is displayed, with a message confirming that the changes have been saved.

Creating a New Member of a PARMS Dataset

To create a new member of a PARMS dataset, perform the following steps:

1. On the TCPaccess Parameters Library List panel, enter **E *uniquemembername*** or **EDIT *uniquemembername*** at the ===> prompt. The Edit TCPaccess PARMS Dataset panel is displayed.
2. Edit the new dataset member, using the method described in the section “Changing a PARMS Member”.

Chapter 8

Managing Open Systems Adapters

This chapter contains the following topics:

- About Open Systems Adapters (OSA)
- Managing OSAs
- Displaying OSA Utilization
- Monitoring OSA Performance
- Listing OSA Devices
- Displaying OSA Configuration

About Open Systems Adapters (OSA)

The IBM Open Systems Adapter (OSA) is a hardware device that combines the functions of a communications controller and a channel, for connecting an OS/390 system to a network. Visibility of OSA resources is provided in the following ways:

- OSA utilization
- OSA performance
- Device list for OSA
- OSA configuration

Managing OSAs

The IP resource monitor provides visibility of the OSAs defined to your region. OSAs are shown as class OSA.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources ------------------------
Command ===>                                                 Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                          Monitor  Alert  Max  Last  Next
   Resource     Class    System   Actual   Status   Count  Sev  Samp  Samp
   DEPT         ASMON    DEPT18   ACTIVE   Ok       0      0    16:17 17:17
   CIPQA18      CIP      DEPT18   ACTIVE   Ok       0      0    16:17 17:17
   CSM          CSM      DEPT18   ACTIVE   Ok       4      2    16:17 17:17
   EE           EE       DEPT18   ACTIVE   Ok       0      0    16:37 16:47
   OSADEX       OSA      DEPT18   ACTIVE   Ok       0      0    16:26 17:26
   OSAEX        OSA      DEPT18   ACTIVE   Ok       0      0    16:26 17:26
   QAS2         OSA      DEPT18   ACTIVE   Ok       0      0    16:26 17:26
   ROTQ18       ROUTER   DEPT18   ACTIVE   Ok       0      0    16:17 17:17
   TCPICSD1     STACK    DEPT18   ACTIVE   Ok       0      0    16:17 17:17
   TCPIP38      STACK    DEPT18   ACTIVE   Ok       0      0    16:17 17:17
   **END**
```

For details of the information displayed, press F1 (Help).

Note: To enable support for an OSA, you must have defined the OSA to NetMaster for TCP/IP. For information about defining an OSA, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

IP Resource Commands

To view the OSA commands available, enter **?** beside an OSA resource.

A panel is displayed, listing the available commands in alphanumeric order, by name, in two groups. Commands that are specific to OSA resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter S beside it.

OSA Commands

The commands specific to OSA resources are:

Command	Description
AL	View alerts for a resource
AM	Activate monitoring
CF	Display OSA configuration settings
D	Display OSA information
DL	Display device list
H	Show performance history
IM	Inactivate monitoring
UM	Update resource monitoring definition

Displaying OSA Utilization

To display OSA utilization and general information, enter **D** (Display) beside an OSA on the IP resource monitor. The Open Systems Adapter Summary panel is displayed.

```
PROD---------------- TCP/IP : Open Systems Adapter Summary -Columns 00001 00079
Command ===>                                                  Scroll ===> PAGE

******************************** TOP OF DATA ********************************
OSA Name ................ TEST
OSA Description ......... test
OSA Type ................ OSA2

Status .................. Online
Collection Status ....... ACTIVE

CHPID ................... B4
CHP %Busy ............... 0.15
Dev. Count .............. 5
****************************** BOTTOM OF DATA ******************************
```

The CHPID % Busy value shows the percentage of time during which the OSA was busy transferring data through the CHPID shown.

For further details of the information displayed and the actions available on the Monitor Open Systems Adapter Performance panel, press F1 (Help).

Monitoring OSA Performance

The Monitor Open Systems Adapter Performance panel provides information and displays graphs of the performance data for the selected OSA. To display this panel, enter **H** (History) beside an OSA on the IP resource monitor.

```
PROD------------- TCP/IP : Monitor Open Systems Adapter Performance------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... OSA2(B4)                Group ... SDD1
     Description ......... Test
     Current Alerts ...... 1
                                    E=Expand C=Contract  S/=Summary D=Detail
                               - Alerts --          Last
    Attribute/Qualifier       Open  Total Samples Sample        Value Type
     |--  AccessOSA/SFapi        1      2       4 15:35              ENUM
     |-- DeviceStatus                  0      10 15:35            - ENUM
     |-- PacketsReceived               0       4 15:35            - COUNT
     |-- PacketsTransmitted            0       4 15:35            - COUNT
     |-- Recoveries                    0       2 15:35            - COUNT
       |-- Port 0                      0       2 15:35            0 COUNT
     |-- TotalOSAErrors                0       4 15:35            - COUNT
    **END**
```

For details of the information displayed and the actions available on the Monitor Open Systems Adapter Performance panel, press F1 (Help).

Note: You can also monitor the performance for an OSA from the OSA Device List. See the section “Listing OSA Devices”.

For more information about the attributes for a monitored resource, see the chapter, “Reporting Real-time Performance”.

Listing OSA Devices

The OSA Device List shows the devices on the OSA that are connected through it to an S/390 system, and provides status and configuration information about these devices. You can access performance data for the OSA and for an OSA device from this device list. To display this list, enter **DL** (Display Device List) beside an OSA on the IP resource monitor (/IPMON).

```
PROD---------------------- TCP/IP : OSA Device List -----------------------------
Command ===>                                                 Scroll ===> PAGE

     CHPID ......... B4                  Name ..........
     Managing LPAR . 1 (STORG1)
     Type .......... Token Ring and Ethernet
     Modes ......... (none configured)
     CU Address .... EB40                Hardware Model  OSA 2
     Code Level .... 6.69                EC Level ...... E13022A
                                                                    H=History
                Home            Device          Device      ------Device-------
    LPAR        Address         Name            Type        Number  AllocatedBy
    STORG1      123.0.88.22     OSA0            LCS         0000    TCPIP38
    STORG1                                                  0001    TCPIP38
    STORG1      123.0.99.22     OSA1            Ethernet    0002    TCPICS52
    STORG1                                                  0003    TCPICS52
    **END**
-------------------------------------------------------------------------------
                                                                    H=History
    Home                                    Net  Device             CHP
    Address         Link Name  Link Type    Num  Status             Status
    123.0.88.22     OSATR0     IBMTR        0    Ready              Online
                                                                    Online
    123.0.99.22     OSAET1     ETHERNET     1    Inactive           Online
                                                                    Online
    **END**
-------------------------------------------------------------------------------
                                                                    H=History
    Home             -----------TRLE ----------
    Address          Resource PortName Status    System
    123.0.88.22      -        -        -         PROD
                     -        -        -         PROD
    123.0.99.22      -        -        -         PROD1
                     -        -        -         PROD1
    **END**
```

To display all the details on the OSA Device List panel, press F11 (Right).

For details of the information displayed on the OSA Device List panel, press F1 (Help).

Monitoring OSA and Device Performance

To monitor the interface workload performance for a device, enter **H** (History) beside the device on the list.

To monitor the performance for the OSA, press **F5** (History). The Monitor Open Systems Adapter Performance panel is displayed.

Displaying OSA Configuration

The OSA Configuration panel provides current configuration values for the hardware and software connected to the OSA. The information comes from the OSA Support Facility (OSA/SF) and falls into these sections:

- General Information is data that describes the OSA hardware, and is about the OS/390 system on which the data was collected.
- Device Information lists the device numbers of the OSA devices, their channel addresses, and their current status.
- Details for Port lists, for each port, the port's hardware type and selected performance data.
- OSA Address Table provides information that allows you to track data transfer through an OSA.

For information about OSA/SF and the OSA address table, see IBM's *OS/390 V2R7.0 OSA/SF User's Guide for OSA-2*.

To display the OSA Configuration panel, enter **CF** (Display OSA Configuration Settings) beside an OSA on the IP resource monitor.

```
PROD---------------------- TCP/IP : OSA Configuration -------Columns 00001 00079
Command ===>                                                  Scroll ===> PAGE

  Channel Path ID (CHPID)   B4
  OSA Name ................ TEST

******************************** TOP OF DATA ********************************

 General information
  SYSPLEX name ................... PLEXNMD
  System name .................... SDD1
  Channel sub-type ............... Token Ring and Ethernet
  Current configuration mode ..... (none configured)
  Hardware model ................. OSA 2
  Number of ports ................ 2
  Channel status ................. Online
  Channel shared? ................ No
  Control unit number ............ EB40
  OSA processor code level ....... 6.80
  EC level .......................
  LPAR of OSA/SF copy doing query  1(STOMD1)
     LPAR of OSA/SF managing this OSA 1(STOMD1)
   Channel node descriptor
     Type number .................. 009676
     Model number ................. 002
     Manufacturer ................. IBM
     Plant of manufacturer ........ 42
     Sequence number .............. 0004283374WK
     Physical identifier .......... 0000
   OSA/SF version ................. V2R1M0
   Query date and time ............ 09/25/2001 17:44:52

 Device information

 Device number  Unit address  Status
 0001           0001          online/allocated
 0002           0002          online/allocated
 0003           0003          online/allocated
 00FE           00FE          online

 Details for port 0
   Port type.............................. TOKENRING
   Status................................. Soft Error, SR Counter Overflow
   Speed.................................. 16Mb
   MAC address............................ 08005A8B382B
   User data.............................. IBM S/390 OSA Token-Ring Port
   Hardware state......................... enabled
   Packets transmitted.................... 6005259
   Packets received....................... 7140044
   Token ring state....................... OPENED
   Token ring open status..............OPEN
   Token ring up-stream neighbour....... 400014211203
   Token ring line errors................. 0
   Token ring burst errors................ 0
   Token ring abort transaction errors   0
   Token ring internal errors ............ 0
   Token ring lost frame errors ......... 0
   Token ring received congestions ..... 0
   Token ring frame copy errors ......... 0
   Token ring soft errors ................ 6
   Token ring hard errors ................ 0
   Token ring signal loss errors ....... 0
   Token ring transmitted beacons ....... 0
   Token ring recoveries ................. 0
   Token ring lobe wire faults ......... 0
   Token ring removals received ......... 0
   Token ring single stations ........... 0
   Token ring full duplex errors ....... 0
```

```
Details for port 1
  Port type...................... ETHERNET
  Status......................... Open
  Speed.......................... 10Mb
  MAC address.................... 10005AD11C34
  User data...................... IBM S/390 OSA Ethernet Port
  Hardware state................. enabled
  Packets transmitted............ 0
  Packets received............... 866647
  Ethernet alignment received erro 0
  Ethernet single collisions..... 0
  Ethernet multiple collisions.... 0
  Ethernet deferred transmissions. 0
  Ethernet late collisions........ 0
  Ethernet excessive collisions... 0
  Ethernet carrier sense errors... 0

OSA address table

LPAR          CHPID  CU number  Device number  Unit address  Channel status
1(STOMD1)     00B4   EB40       0000           0000          Configured
-             -      -          0001           0001          Configured
-             -      -          0002           0002          Configured
-             -      -          0003           0003          Configured
****************************** BOTTOM OF DATA*********************************
```

For details of the information displayed, press F1 (Help).

Chapter 9

Managing Cisco Channel Cards

This chapter contains the following topics:

- About Cisco Channel Cards
- Diagnosing Telnet Connection Problems
- Managing Channel Cards
- Displaying Channel Card Information
- Displaying TN3270 Server Information
- Displaying the TN3270 Server Log
- Displaying CLAW Information
- Displaying CLAW Subchannel Information
- Displaying TCP Offload Information
- Displaying CSNA Information
- Displaying Internal LAN Information
- Monitoring Channel Card Performance

About Cisco Channel Cards

The Cisco Mainframe Channel Connection (CMCC) is supported on the Channel Interface Processor (CIP) and the Channel Port Adapter (CPA). This manual refers to the CIP and CPA as Cisco channel cards.

The Cisco channel card has many functions, some of which are:

- Interconnection controller and providing TCP/IP connectivity for the mainframe
- LAN based SNA connectivity to PUs
- TN3270 server, saving S/390 CPU cycles on OS/390 by running on the channel card

To support the use of Cisco channel cards in your environment, NetMaster for TCP/IP provides you with the ability to do the following:

- List TN3270 Telnet connections by specifying IP address, LU name, and application name.
- Obtain a history of important events on the LU.
- Obtain SNA data about the connection.
- Create alerts automatically in the alert monitor when user-specified thresholds are exceeded.
- Obtain TN3270 server status information.
- Monitor the behavior of the channel card and its components.
- Monitor the performance and health of the channel card by providing indicators such as:
  - CPU, memory, and DMA utilization
  - Transfer rates on CLAW links
  - Error rates on channel interfaces
  - TN3270 server users and free LU counts.
- Display graphs of recent samples of performance data (collected over the last 24-hour period).
- Display PC-based graphs and printed reports of performance data (collected over days, weeks, and months) by using a reporting tool.

Monitoring Channel Cards

The status of the channel card and its associated components may provide you with the necessary information to help you tune the network and resolve problems such as:

- Why the network appears to be running slowly
- Why users cannot establish a session
- Why a certain part of the network is totally isolated
- Why file transfers are taking an unusually long time

Diagnosing Telnet Connection Problems

A channel card appears as a type of link on Telnet connection lists. Since NetMaster for TCP/IP can support multiple systems, a Telnet connection list can display multiple channel cards, or a mix of channel card and TCP/IP on OS/390 links.

```
PROD------------------- TCP/IP : Telnet Connection List ---------Link: CMCC7505
Command ===>                                                    Scroll ===> CSR

    Line 1 of 2                                  Refresh Every ... ___  Seconds
     P=Ping T=TraceRoute D=VTAM Display SL=Session List NL=Lookup S=View Z=Drop
                   MT=Mini Trace TPA=Transaction Path Analyzer L=Log ?=Actions
                                                          Bytes    Bytes
    Foreign Host    LU Name  Applname Status              Out       In
    123.0.92.70     SCC70201 TEST1    Establshd        69810    10606
    123.0.92.70     SCC70204 TEST1    Establshd         1198      196
    **END**
```

To diagnose Telnet connection problems with a channel card, you can display a Telnet LU mini trace from the Telnet Connection List panel.

To display a selection list of the actions you can apply to a listed connection, enter **?** beside it.

Viewing a Telnet LU Mini Trace

The Telnet LU mini trace displays a list of current events received by the TN3270 server. To display the TCP/IP : Cisco Telnet LU Mini Trace panel, type **MT** next to the required LU, and press ENTER.

```
PROD---------------- TCP/IP : Cisco TN3270 LU Mini Trace --------------CMCC7505
Command ===>                                                 Scroll ===> CSR

.---------------------.  .------------------------.  .------------------------.
|  Host Application   |  |     TN3270 Server      |  |     Telnet Client      |
| Name    : STNM1     |  | Addr : 123.123.10.35   |  | Addr : 123.0.92.70     |
| BytesOut: 119370    |  | LU   : SCC70201        |  | Type : TN3270E         |
| BytesIn : 6914      |  | State: Act/Sess        |  | Model: 3278S4E         |
'---------------------'  '------------------------'  '------------------------'

    Event Code   Host              PU          LU              Client
      1    15                                  <----- Connect ----
      2    12      --- Reply PSID +ve Rsp ----->
      3    3       --- Req(ACTLU) ->
      4    4       --- Req(BIND) -------------->
      5    8       --- Req(SDT) --------------->
      6    17                                  <-- Rsp (timing) --
      7    0
```

For details of the information displayed, press F1 (Help).

Managing Channel Cards

You can use the IP resource monitor to manage channel cards. The features include:

- Integration with other NetMaster for TCP/IP and SNA functions
- User access to multiple systems from a single point

Channel cards are shown as class CIP.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources ------------------------
Command ===>                                                 Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                        Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual   Status   Count  Sev  Samp  Samp
    DEPT         ASMON    DEPT18   ACTIVE   Ok       0      0    16:17 17:17
    CMCC7505     CIP      DEPT18   ACTIVE   Ok       0      0    16:17 17:17
    CSM          CSM      DEPT18   ACTIVE   Ok       4      2    16:17 17:17
    EE           EE       DEPT18   ACTIVE   Ok       0      0    16:37 16:47
    OSADEX       OSA      DEPT18   UNKNOWN  -        -      -    16:26 17:26
    OSAEX        OSA      DEPT18   UNKNOWN  -        -      -    16:26 17:26
    QAS2         OSA      DEPT18   UNKNOWN  -        -      -    16:26 17:26
    ROTQ18       ROUTER   DEPT18   ACTIVE   Ok       0      0    16:17 17:17
    TCPICSD1     STACK    DEPT18   ACTIVE   Ok       0      0    16:17 17:17
    TCPIP38      STACK    DEPT18   ACTIVE   Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

Note: To enable support for a Cisco channel card, you must have defined the channel card to NetMaster for TCP/IP. For information about defining a channel card, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

IP Resource Commands

To view the channel card commands available, enter **?** beside a CIP resource.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to channel card resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** beside it.

Channel Card Commands

The commands specific to CIPs are:

Command	Description
AL	View alerts for a resource
ALH	View alerts history for a resource
AM	Activate monitoring
CI	Channel information
CL	CLAW information
CS	CLAW subchannel list
D	Display general information
H	Show performance history
HI	Host interface list
IM	Inactivate monitoring
LAN	Internal LAN information
OF	TCP offload information
PU	TN3270 PU information
SI	System information
TN	Start a Telnet connection
TNI	TN3270 server information
TNL	TN3270 server log
UM	Update resource monitoring definition
WT	Telnet workload data

Displaying Channel Card Information

By showing the general health and status information for the channel card, the Cisco Channel Card Information panel allows you to detect problems with the channel card on the router.

To display the Cisco Channel Card Information panel, enter **D** (Display General Information) beside a CIP on the IP resource monitor.

```
PROD-------------- TCP/IP : Cisco Channel Card Information ------------CMCC7505
Command ===>                                                  Scroll ===> CSR

Slot Number .... 2                . Resource Usage ---------- 100% -----------.
Up Time ........ 6 Days 16:39:00  |    Memory ==21%                50Mb Free  |
IOS Software ... 11.2(10)         | CPU: 1min 1%                   1%         |
Microcode ...... 22.25            |      5min 1%                   1%         |
Hardware ....... 5.0              |     60min 0%                   0%         |
Model .......... Cisco 7505       | DMA: 1min 1%                   1%         |
Ch. 0 Status ... Online           |      5min 0%                   0%         |
                                  |     60min 0%                   0%         |
                                  '-----------------------------------------'
                                                          S/D=Display Application
   Application                Rev  Compile Information
   802                        0    Compiled by admin1 on Tue 14-Mar-2000 15:07
   CSNA                       0    Compiled by admin1 on Tue 14-Mar-2000 15:07
   ECA                        0    Compiled by admin1 on Tue 14-Mar-2000 15:08
   TCP OFFLOAD                0    Compiled by admin1 on Tue 14-Mar-2000 15:07
   TCPIP                      0    Compiled by admin1 on Tue 14-Mar-2000 15:07
   TN3270 Server              0    Compiled by admin1 on Tue 14-Mar-2000 19:01
   **END**
```

For details of the information displayed and the actions available on the Cisco Channel Card Information panel, press F1 (Help).

Displaying Application Information

Application information displays are available for applications specified on the Cisco Channel Card Information panel. The supported applications are:

- TN3270 server
- CSNA
- CLAW (TCP datagram)
- TCP Offload

Note: Not all applications support these additional application information displays.

To display application information, in the Application column on the Cisco Channel Card Information panel, enter **S** next to an application. The selected application information panel is displayed.

Details about application information display panels are given in later sections of this chapter.

Starting a Telnet Connection to the Router

To start a Telnet full-screen connection to a router containing a channel card, enter **TN** (Start a Telnet Connection) beside a CIP on the IP resource monitor. The TCP/IP : Telnet panel is displayed.

Note: You can also start a Telnet connection by pressing F4 on the Server Information, Channel Information, PU List, LU List, and CLAW panels.

Displaying Channel Information

The TCP/IP : Cisco Channel Information panels provide details, statistics, and any error indications for devices on the channel card interfaces.

To display the Cisco Channel Information panel, enter **CI** (Channel Information) beside a CIP on the IP resource monitor. To see additional information, press F11 (Right).

```
PROD---------------- TCP/IP : Cisco Channel Information -------------CMCC7505
Command ===>                                                  Scroll ===> CSR

. Channel 0 ---------------------------+ Channel 1 ---------------------------.
| Board Type ... Escon                 | Board Type ... NOT-CONFIGURED         |
| Status ....... Online                | Status .......                        |
| Last Failure . ***                   | Last Failure .                        |
| Incidents: 0      SignalLoss: 0      | Incidents:        SignalLoss:         |
| CodeVioln: 0      SeqTimeOut: 0      | CodeVioln:        SeqTimeOut:         |
| NotOperSq: 0      InvalidSeq: 0      | NotOperSq:        InvalidSeq:         |
| Load: 1min ... 1%                    | Load: 1min ...                        |
|       5min ... 0%                    |       5min ...                        |
|       60min .. 0%                    |       60min ..                        |
'--------------------------------------+---------------------------------------'
      Path  Device             Device  Device          Selective  System
   Ch Num   Num     Function  Connects  Errors  Cancels    Resets  Resets
   0  B511  00      CLAW            32       0        3         0       8
   0  B511  01      CLAW            28       0        0         0       8
   0  B511  02      CSNA        116861       0        5         0       8
   0  B511  04      Offload         17       0        0         0       8
   0  B511  05      Offload         17       0        0         0       8
-------------------------------------------------------------------------------
      Path  Device           Command   Blocks  Control Unit
   Ch Num   Num     Function  Retries  Dropped        Busies
   0  B511  00      CLAW            7        0             0
   0  B511  01      CLAW            0        0             0
   0  B511  02      CSNA        22757        0             0
   0  B511  04      Offload         0        0             0
   0  B511  05      Offload         0        0             0
-------------------------------------------------------------------------------
      Path  Device           Last Sense  Last Sense
   Ch Num   Num     Function  Data        Time
   0  B511  00      CLAW      0080         4 Days 11:41:30
   0  B511  01      CLAW      0080         4 Days 11:41:30
   0  B511  02      CSNA      0080         4 Days 11:41:30
   0  B511  04      Offload   0080         4 Days 11:41:30
   0  B511  05      Offload   0080         4 Days 11:41:30
```

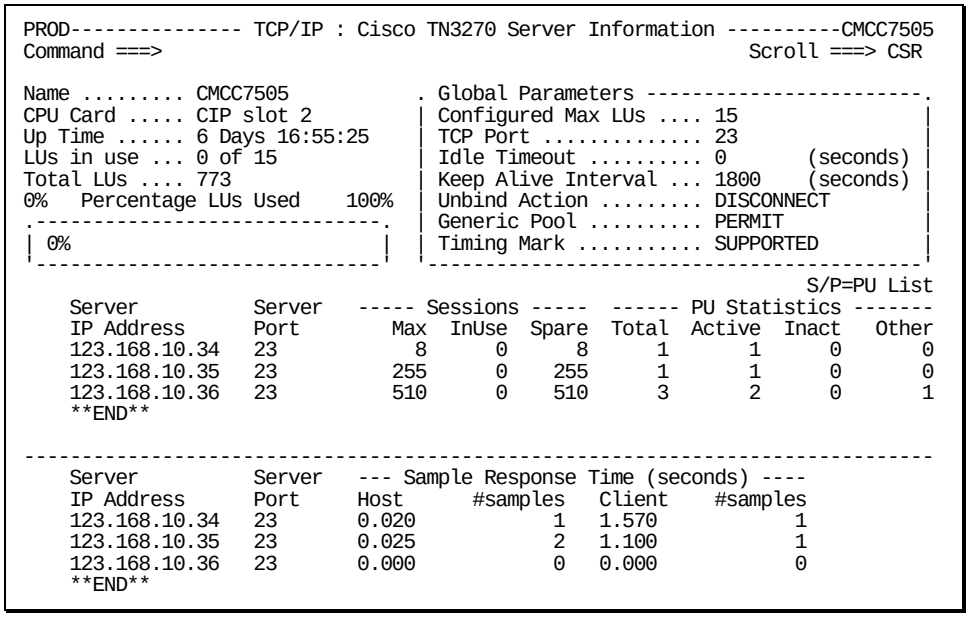
For details of the information displayed on the Cisco Channel Information panel, press F1 (Help).

Displaying TN3270 Server Information

The TCP / IP : Cisco TN3270 Server Information panels allow you to detect the cause of problems with TN3270 server access (for example, an SNA connectivity problem). The panels provide information such as status, configuration, and statistics related to the TN3270 server.

To display the Cisco TN3270 Server Information panel, enter **TNI** (TN3270 Server Information) beside a CIP on the IP resource monitor.

To see additional information on the panel, press F11 (Right).



```
PROD--------------- TCP/IP : Cisco TN3270 Server Information ----------CMCC7505
Command ===>                                                 Scroll ===> CSR

Name ......... CMCC7505           . Global Parameters ------------------------.
CPU Card ..... CIP slot 2          | Configured Max LUs .... 15                |
Up Time ...... 6 Days 16:55:25     | TCP Port .............. 23                |
LUs in use ... 0 of 15             | Idle Timeout .......... 0       (seconds) |
Total LUs .... 773                 | Keep Alive Interval ... 1800    (seconds) |
0%   Percentage LUs Used    100%   | Unbind Action ......... DISCONNECT        |
.------------------------------.   | Generic Pool .......... PERMIT            |
| 0%                           |   | Timing Mark ........... SUPPORTED         |
'------------------------------'   '-------------------------------------------'
                                                                    S/P=PU List
    Server          Server    ----- Sessions -----  ------ PU Statistics -------
    IP Address      Port        Max  InUse  Spare  Total  Active  Inact   Other
    123.168.10.34   23            8      0      8      1       1      0       0
    123.168.10.35   23          255      0    255      1       1      0       0
    123.168.10.36   23          510      0    510      3       2      0       1
    **END**

-------------------------------------------------------------------------------
    Server          Server    --- Sample Response Time (seconds) ----
    IP Address      Port      Host      #samples   Client    #samples
    123.168.10.34   23        0.020            1   1.570            1
    123.168.10.35   23        0.025            2   1.100            1
    123.168.10.36   23        0.000            0   0.000            0
    **END**
```

For details of the information displayed and actions available on the Cisco TN3270 Server Information panel, press F1 (Help).

Function Keys on the Cisco TN3270 Server Information Panel

You can use the following functions keys on the TCP / IP : Cisco TN3270 Server Information panel:

F4 (Telnet)—Start a Telnet connection to the channel card.

F5 (Log)—Display the TN3270 server log.

Listing PUs for a Server

The TCP/IP : Cisco TN3270 PU List allows you to check the PU status and configuration on both the channel card side and the VTAM side.

To display the Cisco TN3270 PU List, from the TCP/IP : Cisco TN3270 Server Information panel, type **S** next to the selected TN3270 server, or type **PU** next to a CIP device.

```
PROD-------------------- TCP/IP : Cisco TN3270 PU List ----------------CMCC7505
Command ===>                                                 Scroll ===> CSR

CIP Name ............ CIPSPPU
Server IP Address ... 123.200.110.194
                    P=Ping T=TraceRoute S/L=LU List D=VTAM Display H=SmartHelp
    TN3270    SNA
    PU Name   PU Name   Status    Server IP Address  Idblk.Idnum  Type
    SCC701    SCC701    Active    123.123.123.123    05D.00081    Direct
    SCC702    SCC702    Active    123.123.123.123    05D.00082    Direct
    **END**
-------------------------------------------------------------------------------
CIP Name ............ CIPSPPU
Server IP Address ... 123.200.110.194
    TN3270    SNA
    PU Name   PU Name   Status    LU Seed  LSAP  RSAP  RMAC
    SCC701    SCC701    Active    SCC701   20    04    400000008001
    SCC702    SCC702    Active    SCC702   24    04    400000008001
    **END**
```

For details of the information displayed and actions available on the Cisco TN3270 PU List, press F1 (Help).

Function Keys on the Cisco TN3270 PU List

You can use the following functions keys on the Cisco TN3270 PU List panel:

F4 (Telnet)—Start a Telnet connection to the channel card.

F5 (Log)—Display the TN3270 server log.

Listing LUs for a PU

The Cisco TN3270 LU List allows you to detect any problems with LUs attached to the TN3270 server by a PU.

To display the Cisco TN3270 LU List, from the Cisco TN3270 PU List, type **S** next to the selected PU and press ENTER.

```
PROD------------------- TCP/IP : Cisco TN3270 LU List -----------------CMCC7505
Command ===>                                                  Scroll ===> CSR

Server IP Address ... 123.123.123.123
PU name ............. SCC701
 P=Ping T=TraceRoute S/D=VTAM Display SL=SessList NL=Lookup V=View MT=Minitrace
    TN3270    SNA                          Client           Client    Client
    LU Name   LU Name   Status    LocAddr  Address          Port      Type
    SCC70102  SCC70102  Active    2
    SCC70103  SCC70103  Active    3
    SCC70104  SCC70104  Active    4
    SCC70105  SCC70105  Active    5
    SCC70106  SCC70106  Active    6
    **END**
-------------------------------------------------------------------------------
Server IP Address ... 123.123.123.123
PU name ............. SCC701
 P=Ping T=TraceRoute S/D=VTAM Display SL=SessList NL=Lookup V=View MT=Minitrace
    TN3270    SNA                          Client
    LU Name   LU Name   Status    LocAddr  Model
    SCC70102  SCC70102  Active    2
    SCC70103  SCC70103  Active    3
    SCC70104  SCC70104  Active    4
    SCC70105  SCC70105  Active    5
    SCC70106  SCC70106  Active    6
    **END**
```

For details of the information displayed and actions available on the Cisco TN3270 LU List, press F1 (Help).

Function Keys on the Cisco TN3270 LU List

You can use the following function keys on the TCP/IP : Cisco TN3270 LU List panel:

F4 (Telnet)—Start a Telnet connection to the channel card.

F5 (Log)—Display the TN3270 server log.

Displaying the TN3270 Server Log

The TN3270 Server Log provides a history of TN3270 server activities. This allows you to diagnose connection problems by using information about connections that are no longer active. You can also diagnose general problems by looking for additional error messages in the log.

The log contains the following types of messages:

- Status and error messages from the TN3270 server about the server software
- Messages about individual connections

You must have the channel card defined with active logging. For information, see the chapter, “Setting Up IP Resource Monitoring” in the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

To display the TN3270 Server Log, enter **TNL** (TN3270 Server Log) beside a CIP on the IP resource monitor.

Note: You can also display the TN3270 Server Log by pressing F5 (Log) from the Cisco TN3270 PU List, the Cisco TN3270 LU List, or the Cisco TN3270 Server Information panel.

```
PROD--------------- TN3270 Server Log : THU 09-AUG-2001 ----------Line 24 of 40
Command ===>                                                  Scroll ===> CSR
IPCP1804 Channel card initialized on THU 21-JUN-2001 at 00:28:12.
Time     Log Data
01:30:55 IPCP1515 Connection started. Client 123.35.122.115:1097 LU FTI.SC70303
01:30:56 IPCP1510 Bind received. Client 123.35.122.115:1097 LU FTI.SC703030 PU
01:30:56 IPCP1599 LU-LU Session started. Client 123.35.122.115:1097 LU FTI.SC70
01:30:56 IPCP1515 Connection started. Client 123.35.122.90:1437 LU SC702003 Mod
01:30:57 IPCP1510 Bind received. Client 123.35.122.90:1437 LU SC702003 PU  Para
01:30:57 IPCP1599 LU-LU Session started. Client 155.35.122.90:1437 LU SC702003
01:30:58 IPCP1596 Disconnected Client 123.35.122.85:1206 From LU SC702002 Reaso
01:31:03 IPCP1515 Connection started. Client 155.35.122.85:1249 LU SC702001 Mod
01:31:03 IPCP1510 Bind received. Client 123.35.122.85:1249 LU SC702001 PU  Para
01:31:03 IPCP1599 LU-LU Session started. Client 155.35.122.85:1249 LU SC702001
01:31:04 IPCP1596 Disconnected Client 123.35.122.115:1063 From LU FTI.SC703005
01:31:05 IPCP1596 Disconnected Client 123.35.122.90:1175 From LU SC702004 Reaso
01:31:09 IPCP1515 Connection started. Client 123.35.122.90:1438 LU SC702013 Mod
01:31:10 IPCP1510 Bind received. Client 123.35.122.90:1438 LU SC702013 PU  Para
01:31:10 IPCP1599 LU-LU Session started. Client 123.35.122.90:1438 LU SC702013
01:32:22 IPCP1596 Disconnected Client 123.35.122.115:1096 From LU FTI.SC703014
01:50:41 IPCP1596 Disconnected Client 123.35.122.86:1069 From LU FTI.SC703001 R
******************************** END-OF-LOG ********************************
 F1=Help      F2=Split     F3=Exit      F4=Exit      F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right
```

For information about the column fields, or about locating information in the TN3270 log, press F1 (Help).

For help on a message in the log, position the cursor on the message line and press F1.

Displaying CLAW Information

The Cisco CLAW Information panels provide you with channel details, statistics, configuration, and any error indications for the Common Link Access to Workstation (CLAW).

This information allows you to manage the CLAW support on the Cisco channel card.

To display the Cisco CLAW Information panel, enter **CL** (CLAW Information) beside a CIP on the IP Resource monitor.

For ESCON channels, you can also display CLAW subchannel information. See the section “Displaying CLAW Subchannel Information”.

```
PROD------------------ TCP/IP : Cisco CLAW Information ----------------CMCC7505
Command ===>                                                  Scroll ===> CSR

. Channel 0 ---------------------------+ Channel 1 ---------------------------.
| Board Type ... Escon                 | Board Type ... NOT-CONFIGURED         |
| Status ....... Online                | Status .......                        |
| Last Failure . ***                   | Last Failure .                        |
| Incidents: 0      SignalLoss: 0      | Incidents:        SignalLoss:         |
| CodeVioln: 0      SeqTimeOut: 0      | CodeVioln:        SeqTimeOut:         |
| NotOperSq: 0      InvalidSeq: 0      | NotOperSq:        InvalidSeq:         |
'--------------------------------------+---------------------------------------'
Common Link Access to Workstation (CLAW) Statistics & Configuration Information
       Path Dev            -----Blocks Read-----  ---Blocks Written----
    Ch Num  Num Claw Conn  Success Dropped %Drop  Success Dropped %Drop
    0  B511 00  0    Yes        11       7    38        0       0     0
    0  B511 00  1    Yes         0       0     0        0       0     0
    0  B511 01  0    Yes         0       0     0        8       0     0
    0  B511 01  1    Yes         0       0     0        0       0     0
    0  B511 04  0    No          0       7   100        0       0     0
    0  B511 04  1    No          0       0     0        0       0     0
--------------------------------------------------------------------------------
Common Link Access to Workstation (CLAW) Statistics & Configuration Information
       Path Dev         Bytes    Bytes  Buffer Get
    Ch Num  Num Claw     Read  Written     Retries
    0  B511 00  0         352        0           0
    0  B511 00  1           0        0           0
    0  B511 01  0           0      256           0
    0  B511 01  1           0        0           0
    0  B511 04  0           0        0           0
    0  B511 04  1           0        0           0
--------------------------------------------------------------------------------
Common Link Access to Workstation (CLAW) Statistics & Configuration Information
       Path Dev                      Host     Device   Host     Device   B'cast
    Ch Num  Num Claw IP Address      Name     Name     Appl'n   Appl'n   Enable
    0  B511 00  0    123.168.10.18   STOMD1   CIP0     TCPIP    TCPIP    No
    0  B511 00  1    123.168.10.18   STOMD1   CIP0     TCPIP    TCPIP    No
    0  B511 01  0
    0  B511 01  1
    0  B511 04  0
    0  B511 04  1
```

For details of the information displayed on the Cisco CLAW Information panel, press F1 (Help).

Displaying CLAW Subchannel Information

The Cisco CLAW Subchannel List panels provide you with subchannel details and statistics for Common Link Access to Workstation (CLAW) links. These details include the following:

- Channel utilization percentages
- Transfer rates on CLAW links
- TCP/IP stack names
- System names
- Channel path IDs

This information is available from two perspectives:

- From the channel card point of view, where the CLAW subchannels are known and you want information about the host channel usage information (for example, what channels are being used by CLAW links to this channel card and how heavily utilized they are)
- From the host channel point of view, where the host channels are known and you want information about the CLAW and other usage for those channels (for example, which devices are using CHPID 10 on PRD0)

Note: Some information on these panels is available only if the TCP/IP stack to which the CLAW link is defined is being monitored by one of the following systems:

- The local NetMaster for TCP/IP region
- A NetMaster for TCP/IP system that is linked to the local region

This applies to the following fields:

- Channel path identifier
- Percentage utilization
- System
- TCP/IP started task

To display the Cisco CLAW Subchannel List, enter **CS** (CLAW Subchannel List) beside a CIP on the IP resource monitor (/IPMON).

CLAW Subchannel List by Card

```
PROD---------------- TCP/IP : Cisco CLAW Subchannel List --------------CMCC7505
Command ===>                                                 Scroll ===> PAGE

                Target          Ch         Read      Write     CHP   Host
    Channel Card IP Address     ID       MB/sec     MB/sec   Util%   Channel
    CMCC1        123.156.78.18  0         0.000      0.000       -   -
    CMCC1        123.156.78.21  0         0.000      0.000    1.46   SYS1.10
    CMCC1        123.156.78.22  0         0.000      0.000       -   -
    CMCC1        123.156.78.24  0         0.000      0.000       -   -
    **END**
-------------------------------------------------------------------------------
                Target               Bytes       Bytes
    Channel Card IP Address            Read     Written
    CMCC1        123.156.78.18      61.494M     17.940M
    CMCC1        123.156.78.21     379.908M    366.494M
    CMCC1        123.156.78.22      83.160M    156.161M
    CMCC1        123.156.78.24     708.608K  10638.336K
    **END**
-------------------------------------------------------------------------------
                Target                Read       Write      Buffer
    Channel Card IP Address        Blks Drop   Blks Drop   Get Retry
    CMCC1        123.156.78.18            42           0           0
    CMCC1        123.156.78.21            42           0           0
    CMCC1        123.156.78.22            47           0           0
    CMCC1        123.156.78.24            47           0           0
    **END**
-------------------------------------------------------------------------------
                Target          Ch                      CHP  TCPIP
    Channel Card IP Address     ID   Path  Dev  System ID   Jobname
    CMCC1        123.156.78.18  0    B511  00   -      -    -
    CMCC1        123.156.78.21  0    B511  06   SYS1   10   TCPICS52
    CMCC1        123.156.78.22  0    C722  50   -      -    -
    CMCC1        123.156.78.24  0    C722  52   -      -    -
    **END**
```

From this display, press F4 to switch to the view by host.

TCP/IP : Cisco CLAW Subchannel List by Host

```
PROD---------------- TCP/IP : Cisco CLAW Subchannel List --------------CMCC7505
Command ===>                                                  Scroll ===> PAGE

    Host                          Target               Read      Write     CHP
    Channel Dev  Channel Card     IP Address         MB/sec     MB/sec   Util%
    -       00   CMCC1            123.156.78.18       0.000      0.000      -
    -       50   CMCC1            123.156.78.22       0.000      0.000      -
    -       52   CMCC1            123.156.78.24       0.000      0.000      -
    SYS1.10 -    Unknown Device   0300                   -          -    0.14
    SYS1.10 -    Unknown Device   0302                   -          -    0.14
    SYS1.10 -    Unknown Device   0304                   -          -    0.14
    SYS1.10 06   CMCC1            123.156.78.21       0.000      0.000    0.14
    SYS1.10 -    Unknown Device   0322                   -          -    0.14
    **END**
-------------------------------------------------------------------------------
    Host                  Bytes       Bytes        Read       Write      Buffer
    Channel Dev            Read     Written   Blks Drop   Blks Drop   Get Retry
    -       00          2.344M      21.300M         282           0           0
    -       50        111.015M      78.504M       22606           0           0
    -       52        339.014M     289.613M         449           0           0
    SYS1.10 -                -           -           -           -           -
    SYS1.10 -                -           -           -           -           -
    SYS1.10 -                -           -           -           -           -
    SYS1.10 08           1.169G      3.447G         367           0           0
    SYS1.10 -                -           -           -           -           -
    **END**
-------------------------------------------------------------------------------
    Host                          Target          Ch         TCPIP
    Channel Dev  Channel Card     IP Address      ID   Path  Jobname
    -       00   CMCC1            123.156.78.18   0    C711  -
    -       06   CMCC1            123.156.78.18   0    C711  -
    -       54   CMCC1            123.156.78.18   0    C722  -
    SYS1.10 -    Unknown Device   0300            -    -     -
    SYS1.10 -    Unknown Device   0302            -    -     -
    SYS1.10 -    Unknown Device   0304            -    -     -
    SYS1.10 08   CMCC1            123.156.78.18   0    C711  TCPICSD1
    SYS1.10 -    Unknown Device   0320            -    -     -
   **END**
```

For details of the information displayed and actions available on the Cisco CLAW Subchannel List, press F1 (Help).

Sorting Entries on the Cisco CLAW Subchannel List

You can use the SORT command to display the CLAW Subchannel List in a sort order other than the default order of channel card or host.

The operand values for the command are associated with the column heading of the column that you want to sort by. For example, enter **SORT DEV** to sort the list by the device.

Note: You can enter **SORT ?** to display a selection list of sort fields.

Displaying TCP Offload Information

The Cisco TCP Offload Information panels provide you with details, statistics, and any error indications for the Cisco channel card TCP offload. This information allows you to manage the TCP offload support on the Cisco channel card.

To display the Cisco TCP Offload Information panel, enter **OF** (TCP Offload Information) beside a CIP on the IP resource monitor (/IPMON).

```
PROD------------- TCP/IP : Cisco TCP Offload Information -------------CMCC7505
Command ===>                                                 Scroll ===> CSR

. Channel 0 ---------------------------+ Channel 1 ---------------------------.
| Board Type ... Escon                 | Board Type ... NOT-CONFIGURED         |
| Status ....... Online                | Status .......                        |
| Last Failure . ***                   | Last Failure .                        |
| Incidents: 0      SignalLoss: 0      | Incidents:        SignalLoss:         |
| CodeVioln: 0      SeqTimeOut: 0      | CodeVioln:        SeqTimeOut:         |
| NotOperSq: 0      InvalidSeq: 0      | NotOperSq:        InvalidSeq:         |
| Load: 1min ... 1%                    | Load: 1min ...                        |
|       5min ... 0%                    |       5min ...                        |
|       60min .. 0%                    |       60min ..                        |
'--------------------------------------+---------------------------------------'
                                          TCP Offload Configuration Information
      Path  Device                     Host      Device    Broadcast
   Ch Num   Num     IP Address       Name      Name      Enable
   0  B511  04      123.168.10.19    TCPIP     TCPIP     No
   0  B5F0  F0      123.168.10.20    TCPIP     TCPIP     No
   **END**
-------------------------------------------------------------------------------
                                          TCP Offload Configuration Information
      Path  Device                    Host         Device
   Ch Num   Num     IP Address       Application  Application
   0  B511  04      123.168.10.19    TCPIP        TCPIP
   0  B5F0  F0      123.168.10.20    TCPIP        TCPIP
   **END**
-------------------------------------------------------------------------------
                                          TCP Offload Configuration Information
      Path  Device                    API Host     API Device
   Ch Num   Num     IP Address       Application  Application
   0  B511  04      123.168.10.19    HLINK        DLINK
   0  B5F0  F0      123.168.10.20    HLINK2       DLINK2
   **END**
```

For details of the information displayed on the Cisco TCP Offload Information panels, press F1 (Help).

Displaying CSNA Information

The TCP/IP : Cisco CSNA Information panels provide you with details, statistics, and any error indications for the SNA support on the Cisco channel card.

This information allows you to manage the Cisco Systems Network Architecture (SNA) support on the channel card.

To display the Cisco CSNA Information panel, enter **SN** (CSNA Information) beside a CIP on the IP resource monitor (/IPMON).

```
PROD----------------- TCP/IP : Cisco CSNA Information ---------------CMCC75055
Command ===>                                                 Scroll ===> CSR

. Channel 0 ---------------------------+ Channel 1 --------------------------.
| Board Type ... Escon                 | Board Type ... NOT-CONFIGURED        |
| Status ....... Online                | Status .......                       |
| Last Failure . ***                   | Last Failure .                       |
| Incidents: 0      SignalLoss: 0      | Incidents:        SignalLoss:        |
| CodeVioln: 0      SeqTimeOut: 0      | CodeVioln:        SeqTimeOut:        |
| NotOperSq: 0      InvalidSeq: 0      | NotOperSq:        InvalidSeq:        |
| Load: 1min ... 1%                    | Load: 1min ...                       |
|       5min ... 0%                    |       5min ...                       |
|       60min .. 0%                    |       60min ..                       |
'--------------------------------------+--------------------------------------'
                                  CSNA Configuration & Statistical Information
      Path  Device                                          Blk Dly  Blk Dly  Max Blk
   Ch Num   Num     Current State  Slow Down State           Time   Length   Length
   0  B511  02      SetupComplete  Normal                     10    20470    20470
   0  B5F0  F4      Closed         Normal                     10    20470    20470
    **END**
-------------------------------------------------------------------------------
                                  CSNA Configuration & Statistical Information
      Path  Device    Blocks   Blocks   Blks Xmit   Blocks Xmit    Blocks Xmit
   Ch Num   Num     Received  Xmitted  Delay Time  Delay Length  MaxBlk Length
   0  B511  02         22797    22795       11306             0              0
   0  B5F0  F4             0        0           0             0              0
   **END**
-------------------------------------------------------------------------------
                                  CSNA Configuration & Statistical Information
      Path  Device     Bytes    Bytes  Bytes Xmit    Bytes Xmit     Bytes Xmit
   Ch Num   Num     Received  Xmitted  Delay Time  Delay Length  MaxBlk Length
   0  B511  02        1.280M   1.590M      1.475M             0              0
   0  B5F0  F4             0        0           0             0              0
   **END**
-------------------------------------------------------------------------------
                                  CSNA Configuration & Statistical Information
     Path  Device  Slowdowns  Slowdowns
  Ch Num   Num      Received       Sent
  0  B511  02             0          0
  0  B5F0  F4             0          0
  **END**
```

For details of the information displayed on the Cisco CSNA Information panel, press F1 (Help).

Displaying Internal LAN Information

The Cisco Internal LAN Information panel allows you to manage the Cisco internal LAN support on the channel card.

To display the Cisco Internal LAN Information panel, enter **LAN** (Internal LAN Information) beside a CIP on the IP resource monitor (/IPMON).

```
PROD-------------- TCP/IP : Cisco Internal LAN Information ------------CMCC7505
Command ===>                                                  Scroll ===> CSR

                                                                     S/=Select
    LAN                          Bridge  Bridge
    Id   LAN Type                Num     Group   Bridge Type
    0    ISO 88025 Token Ring    1       0       Source-Route Only
    **END**
```

For details of the information displayed and action available on the Cisco Internal LAN Information panel, press F1 (Help).

Displaying Internal LAN Adapters

To display the Cisco Internal LAN Adapters panel, at the Internal LAN Information panel, enter **S** next to the required LAN.

```
PROD--------------- TCP/IP : Cisco Internal LAN Adapters --------------CMCC7505
Command ===>                                                  Scroll ===> CSR

Slot Number ..... 2
LAN Id .......... 0
LAN Type ........ ISO 88025 Token Ring
Bridge Number ... 1
Bridge Group .... 0
Bridge Type ..... Source-Route Only
Local Ring ...... 1
Target Ring ..... 80
    Adapter  Adapter
    Number   Name      MAC Address
    0                  400000008001
    1                  400000008002
    **END**
```

For details of the information displayed on the Cisco Internal LAN Information panel, press F1 (Help).

Monitoring Channel Card Performance

You can monitor the performance and health status of a Cisco channel card by accessing the Resource Data List and applying either the S (Summary) or D (Detail) action to an attribute on the list.

The Monitor Channel Card Performance panel allows you to monitor the performance and health status of a Cisco channel card.

To display the Monitor Channel Card Performance panel, enter **H** (History) beside a CIP on the IP resource monitor (/IPMON).

```
PROD---------------- TCP/IP : Monitor Channel Card Performance ----------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... CIPSPPU
     Description ......... Cisco Router
     Current Alerts ...... 2
                                      E=Expand C=Contract  S/=Summary D=Detail
                                 - Alerts --         Last
    Attribute/Qualifier          Open  Total Samples Sample        Value Type
     |-- (no qualifier)             1      8      32 10:34            - GAUGE
     | |-- CPULoad5m                       0       8 10:34            1 GAUGE
     | |-- DMALoad5m                       0       8 10:34            1 GAUGE
     | |-- MemUsedPercent             1    8       8 10:34           23 GAUGE
     | |-- TN3270FreeLUs                   0       8 10:34           84 GAUGE
     |-- Channel 0                    1    8      40 10:34            - GAUGE
     |-- CLAW Total                      0      48 10:34            - GAUGE
     |-- CMCC Channel                    0      16 10:34            - GAUGE
     |-- 123.199.199.191                 0      48 10:34            - GAUGE
     |-- 123.199.199.192                 0      48 10:34            - GAUGE
     |-- 123.199.199.193                 0      48 10:34            - GAUGE
     |-- 123.199.199.194                 0      48 10:34            - GAUGE
     |-- 123.199.199.195                 0      48 10:34            - GAUGE
 F1=Help      F2=Split     F3=Exit      F4=Expand    F5=Find      F6=AutoRfsh
 F7=Backward  F8=Forward   F9=Swap                  F11=Right    F12=ByAttr
```

For details of the information displayed and the actions available on the Monitor Channel Card Performance panel, press F1 (Help).

The information sampled is controlled by the NetMaster for TCP/IP system administrator and can include:

- Channel card CPU use
- Channel card memory use
- DMA load (DMA communicates between the channel card and route processor)
- Channel load
- Channel errors
- TN3270 usage

For ESCON channels, the following additional information is available:

- Channel utilization (in bytes or percentages)
- CLAW read and write statistics

Chapter

10

Managing 2216 Routers

This chapter contains the following topics:

- Managing 2216 Routers
- Displaying 2216 Router Information
- Displaying TN3270 Server Information
- Displaying TN3270 PU Information
- Displaying TN3270 LU Information
- Displaying Channel Information
- Monitoring 2216 Router Performance

Managing 2216 Routers

You can use the IP resource monitor to manage 2216 routers and their TN3270 servers that are channel connected to OS/390 mainframe servers.

2216 routers are shown as class ROUTER.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources -------------------------
Command ===>                                                 Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                          Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual  Status   Count  Sev  Samp  Samp
    DEPT         ASMON    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CIPQA18      CIP      DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CSM          CSM      DEPT18   ACTIVE  Ok       4      2    16:17 17:17
    EE           EE       DEPT18   ACTIVE  Ok       0      0    16:37 16:47
    OSADEX       OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    OSAEX        OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    QAS2         OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    2216         ROUTER   DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPICSD1     STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPIP38      STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

Note: To enable support for a 2216 router, you must have defined the 2216 router to NetMaster for TCP/IP. For information about defining the 2216 router, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

IP Resource Commands

To view the 2216 router commands available, enter **?** beside a 2216 router resource.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to 2216 router resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** beside it.

2216 Router Commands

The commands specific to 2216 routers are:

Command	Description
AL	View alerts for a resource
ALH	View alerts history for a resource
AM	Activate monitoring
CI	Channel information
D	Display general information
H	Show performance history
HI	Host interface list
IM	Inactivate monitoring
LU	TN3270 LU information
PU	TN3270 PU information
SI	System information
TN	Start a Telnet connection
TNI	TN3270 server information
UM	Update resource monitoring definition

Displaying 2216 Router Information

The 2216 Router Information panel allows you to perform a quick check of the router's operation. You can check on the following:

- How busy the router is
- What adapters are installed in the router
- The status of each of the router's adapters

To display the 2216 Router Information panel, enter **D** (Display General Information) beside a router on the IP resource monitor (/IPMON).

```
PROD-------------- TCP/IP : 2216 Router Information ----------------------2216
Command ===>

. CPU Usage - 0% ------------------- 100% --.
|    -1 min 0                               |
|    -2 min 0                               |
|    -3 min 0                               |
|    -4 min 0                               |
|    -5 min 0                               |
'-------------------------------------------'

. Slot  I/F  Card type ----------------------- Status -------------------------.
|    1       token-ring-lic280                enabled                          |
|    2       not-present                      not-present                      |
|    3       not-present                      not-present                      |
|    4       not-present                      not-present                      |
|    5       not-present                      not-present                      |
|    6       not-present                      not-present                      |
|    7    1  ethernet-fast-lic288             enabled                          |
|    8    2  escon-lic287                     enabled                          |
'-------------------------------------------------------------------------------'
```

For details of the information displayed and the actions available, press F1 (Help).

Displaying TN3270 Server Information

The 2216 TN3270 Server Information panel displays general information such as the status of the TN3270 server, and allows you to gauge how busy it is, by measuring the number of sessions and the number of bytes transmitted.

To display the 2216 TN3270 Server Information panel, enter **TNI** (TN3270 Server Information) beside a router on the IP resource monitor (/IPMON).

```
PROD-------------- TCP/IP : 2216 TN3270 Server Information ----------------2216
Command ===>                                                  Scroll ===> PAGE

Name ......... 2216               . Functions Supported ----------------------.
Admin Status . Up                  | Y TransmitBinary     Y DataStreamCtl      |
Oper Status .. Up                  | Y TimeMark           Y ScsCtlCodes        |
                                   | Y EndOfRecord        Y Responses          |
                                   | Y TerminalType       Y BindImage          |
                                   | n tn3270Regime       Y SysReq             |
                                   '-----------------------------------------'
     Port -Up-Time- -------LUs------- ----Connections----- -------Bytes--------
                         Max  Used Spare     In Reject   Disc        In        Out
    (all) 41.3 days        1     1     0    339     84    254    3.552M    49.209M
    **END**
```

For details of the information displayed and the actions available, press F1 (Help).

Displaying TN3270 PU Information

The 2216 TN3270 PU List panel lists information about each of the PUs used by the TN3270 server.

To display the 2216 TN3270 PU List panel, enter **PU** (TN3270 PU Information) beside a router on the IP resource monitor (/IPMON).

```
PROD------------------- TCP/IP : 2216 TN3270 PU List ----------------------2216
Command ===>                                                  Scroll ===> PAGE

Router Name ......... 2216
Server IP Address ... 199.0.81.2
                                                          D/S=VTAM Display P=Ping
         PU Name   Status    Server      Idblk.Idnum   Last    --Act-Failures--
                           IP Address                  Change  Num       Reason
      FTI.SCI2CP   active                 077.00000   Startup   0           -
      FTI.SCI201   active                 077.00091  4.9 days   0           -
      FTI.SCI202   active                 077.00092  4.9 days   0           -
      **END**
```

For details of the information displayed and the actions available, press F1 (Help).

Displaying TN3270 LU Information

The 2216 TN3270 LU List displays information about TN3270 sessions serviced by a 2216 router. Such information includes the mapping of IP addresses to LU names and application names. It allows you to investigate problems occurring on any of the listed connections by using the actions shown on the panel.

To display the 2216 TN3270 LU List panel, enter **LU** (TN3270 LU Information) beside a router on the IP resource monitor (/IPMON).

```
PROD------------------- TCP/IP : 2216 TN3270 LU List ----------------------2216
Command ===>                                                 Scroll ===> PAGE

Router name ......... 2216

              D=VTAM Display L=Lookup P/S=Ping SL=SessList T=TraceRoute V=View
     LU Name  Client Address  Session   Idle     Primary  --------Bytes--------
                              State     Time     LU              Out         In
     SCI20102 199.0.91.128    lu-lu     00:00:44 STNM1         13451       4843
     SCI20104 199.0.91.128    lu-lu     00:00:12 SDTSO014      61993       2127
     SCI20107 10.112.2.13     lu-lu     00:00:30 STNM1        289127      40185
     **END**
```

For details of the information displayed and the actions available, press F1 (Help).

Displaying Channel Information

The 2216 Router Channel Information panel displays information about the 2216 router's channel connection to the host. You can check on the following:

- How busy the channel connections are
- What the channel status is
- Which host systems the 2216 router is connected to
- By comparing the amount of activity on the various channel stations, you get an idea of what type of traffic predominates—is it mainly Telnet users or is it mainly TCP/IP that is keeping the 2216 router busy?

ESCON Connection Hierarchy

A three-level hierarchy exists in ESCON connections between a 2216 router and its hosts: port, links, and stations:

- A port identifies an ESCON cable. The fields relevant to a port are: Interface Number, Port Status (In), and Port Status (Out). On the display, all lines that have the same Interface Number refer to the same port.

- Within each port, there are links. Each link identifies a connection between the 2216 router and a particular logical host. Fields relevant to a link are: HLA, CUA, LPAR, and Link Status. On the display, all rows that have the same combination of interface number, HLA, CUA, and LPAR refer to the same link.
- Within each link, there are stations. Fields relevant to stations are: device address, station state, max message size receivable/sendable, packets received ok/received in error/sent, and frames sent. On the display, all rows that have the same combination of interface number, HLA, CUA, LPAR, and device address refer to the same station.

To display the 2216 Router Channel Information panel, enter **CI** (Channel Information) beside a router on the IP resource monitor (/IPMON).

```
PROD------------ TCP/IP : 2216 Router Channel Information ----------------2216
Command ===>                                                 Scroll ===> PAGE

Channel connections to ... 2216

     IF HLA CUA LPAR Dev  -------Port-Status-------- Link         Station
     No             Addr  In        Out             Status       State
      2  B5   0    1  22  inIdle    outEnable       hlpEstab     cpActive
      2  B5   0    2  20  inIdle    outEnable       hlpNotEstab  cpActive
      2  B5   0    2  21  inIdle    outEnable       hlpNotEstab  cpActive
    **END**
------------------------------------------------------------------------------
Channel connections to ... 2216

     IF HLA CUA LPAR Dev   Max-Msg-Size   ----------Packets----------   Frames
     No             Addr     Recv  Send   ReceivdOK RecvdErr      Sent     Sent
      2  B5   0    1  22     4656  4656       84522        0     80739    84491
      2  B5   0    2  20     4656  4656           0        0         0        0
      2  B5   0    2  21     4656  4656           0        0         0        0
    **END**
```

For details of the information displayed and the actions available, press F1 (Help).

Monitoring 2216 Router Performance

You can monitor the performance and health status of a 2216 router by accessing the Monitor 2216 Router Performance panel and applying either the S (Summary) or D (Detail) action to an attribute on the list.

To access the Monitor 2216 Router Performance panel, enter **H** (Show Performance History) beside a router on the IP resource monitor (/IPMON).

```
PROD---------------- TCP/IP : Monitor 2216 Router Performance-----------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... 2216
     Description ......... IBM 2216-400 Multiprotocol Acc
     Current Alerts ...... 0
                                     E=Expand C=Contract  S/=Summary D=Detail
                                - Alerts --          Last
    Attribute/Qualifier         Open  Total Samples Sample        Value Type
     |-- (no qualifier)                0      35 13:11              - GAUGE
     | |-- tn3270BytesIn               0       7 13:11              0 COUNT
     | |-- tn3270BytesOut              0       7 13:11            112 COUNT
     | |-- tn3270LUs                   0       7 13:11              1 GAUGE
     | |-- tn3270LUsSpare              0       7 13:11              0 GAUGE
     | |-- CPULoad                     0       7 13:11              0 GAUGE
     |-- FTI.SCI2CP                    0       7 13:11              - ENUM
     | |-- PUstatus                    0       7 13:11         active ENUM
     |-- FTI.SCI201                    0       7 13:11              - ENUM
     | |-- PUstatus                    0       7 13:11         active ENUM
     |-- FTI.SCI202                    0       7 13:11              - ENUM
     | |-- PUstatus                    0       7 13:11         active ENUM
```

For details of the information displayed and the actions available on the Monitor 2216 Router Performance panel, press F1 (Help).

The sampled information is controlled by the NetMaster for TCP/IP system administrator and can include:

- Adapter status
- Channel status
- 2216 router CPU load
- Interface load
- TN3270 load

For details of the information displayed and the actions available, press F1 (Help).

Chapter

11

Managing Enterprise Extender

This chapter contains the following topics:

- About Enterprise Extender
- Managing Enterprise Extender
- Displaying XCA Major Node Summary
- Displaying XCA Major Node
- Listing Sessions
- Displaying UDP Port Activity
- Monitoring Enterprise Extender Performance

About Enterprise Extender

Enterprise Extender, a feature of IBM's OS/390 and z/OS operating systems, connects SNA clients to the mainframe over an IP backbone by using the UDP protocol.

From an SNA view, Enterprise Extender is a logical link that is defined as an XCA (eXternal Communications Adapter) major node and a switched major node. Each LPAR can have only one active Enterprise Extender XCA major node. The Sessions action provides a view of Enterprise Extender sessions at the SNA node level.

From an IP view, Enterprise Extender is UDP traffic over the IP backbone. The UDP port activity action provides visibility of Enterprise Extender at the UDP port level.

The IP resource monitor allows you to manage Enterprise Extender connections by providing both SNA and IP views of Enterprise Extender communications. It also allows you to monitor areas of Enterprise Extender communications to ensure their services are available.

Managing Enterprise Extender

You can use the IP resource monitor to manage Enterprise Extender.

Enterprise Extender resources are shown as class EE.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources -------------------------
Command ===>                                                 Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                          Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual  Status   Count  Sev  Samp  Samp
    DEPT         ASMON    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CIPQA18      CIP      DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    CSM          CSM      DEPT18   ACTIVE  Ok       4      2    16:17 17:17
    EE           EE       DEPT18   ACTIVE  Ok       0      0    16:37 16:47
    OSADEX       OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    OSAEX        OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    QAS2         OSA      DEPT18   UNKNOWN -        -      -    16:26 17:26
    ROTQ18       ROUTER   DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPICSD1     STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    TCPIP38      STACK    DEPT18   ACTIVE  Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

Note: To enable support for Enterprise Extender, you must have defined Enterprise Extender to NetMaster for TCP/IP. For information about defining Enterprise Extender, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

IP Resource Commands

To view the Enterprise Extender commands available, enter **?** beside an Enterprise Extender resource.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to Enterprise Extender resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** beside it.

Enterprise Extender Commands

The commands specific to Enterprise Extender are:

Command	Description
AL	View alerts for a resource
ALH	View alerts history for a resource
D	Display XCA major node summary
H	Show performance history
IM	Inactivate monitoring
N	XCA major node information
SL	Session list
UA	UDP port activity
UM	Update resource monitoring definition

Displaying XCA Major Node Summary

The XCA Major Node Summary panel displays general information about the XCA major node.

To display the XCA Major Node Summary panel, enter **D** (Display XCA Major Node Summary) beside an EE entry on the IP resource monitor (/IPMON).

```
PROD------------------- TCP/IP : EE XCA Major Node Summary --- Cols 00001 00079
Command ===>                                                  Scroll ===> PAGE

******************************** TOP OF DATA ********************************
XCA Major Node Name ..... EE01XCA

XCA Major Node Status ... ACTIV

TCP/IP Job Name ......... TCPIPC
Local IP Address ........ 123.11.215.17
****************************** BOTTOM OF DATA ******************************
```

For details of the information displayed, press F1 (Help).

Displaying XCA Major Node

The XCA Major Node Information option provides a hierarchical view of the host and the lines associated with the XCA major node.

To display the NCS : Node Display - XCA MAJN panel, enter **N** (XCA Major Node Summary Information) beside an EE entry on the IP resource monitor (/IPMON).

```
PROD--------------------- NCS : Node Display - XCA MAJN ---------------------FTI
Command ==>                                                  Scroll ==> PAGE

Node Name ... EE01XCA                                 Link Name ... PROD----
                            --------------
                           |     HOST     | NET ID.. NET01
    LINES:(10)             |              | OP SYS.. OS390
___ EE01L000 ACTIV     ___ |    SOLVTM1   | SUBAREA. 13
___ EE01L001 ACTIV         ------| |-----  VTAM.... 4.8.0
___ EE01L002 ACTIV         ------| |-----
___ EE01L003 ACTIV         | XCA MAJ NODE | STATUS.. ACTIV
___ EE01L004 ACTIV         |              | DESIRED. ACTIV
___ EE01L005 ACTIV     ___ |   EE01XCA    | MEDIUM.. HPRIP
___ EE01L006 ACTIV         |              | TRACE... NONE
___ EE01L007 ACTIV          --------------  Local IP Addr  199.199.199.199
___ EE01L008 ACTIV
___ EE01L009 ACTIV
    **END**
```

For details of the information displayed and actions available, press F1 (Help).

Displaying Additional Information

From the NCS : Node Display - XCA MAJN panel you can select a resource to display a hierarchical view and additional information about the selected resource. For example, select a line by entering **S** in the input field beside the line you want. The NCS : Node Display - LINE panel is displayed. You can zoom in and out of the views of VTAM resources.

```
PROD---------------------- NCS : Node Display - LINE ----------------------FTI
Command ==>                                                  Scroll ==> PAGE

Node Name ... EE01L008                              Link Name ... SOLV7
                           --------------
                          |    HOST      | NET ID.. NET01
    NETWORK RESOURCES:(1) |              | OP SYS.. OS390
    CN000039 ACTIV    ___ |  SOLVVTM1    | SUBAREA. 13
    **END**               -----| |------  VTAM.... 4.8.0
                          -----| |------
                          | XCA MAJ NODE | STATUS.. ACTIV
                          |              | DESIRED. ACTIV
                      ___ |   EE01XCA    | MEDIUM.. HPRIP
                          -----| |------  TRACE... NONE
                          -----| |------  Local IP Addr  199.199.199.199
                          |    LINE      | STATUS.. ACTIV     LINETYP. DIAL-IN
                          |              | DESIRED. ACTIV     PRCOL... SDLC
                      ___ |  EE01L008    | ANSMODE. ENABLED
                           --------------  LINEGRP. EE01XCAG
```

For details of the information displayed and actions available, press F1 (Help).

From the NCS : Node Display - XCA MAJN panel you can also access status information about a network resource. To display the NCS : SNA Status Code panel, enter **Q** beside the network resource you want.

Listing Sessions

The Enterprise Extender Session List displays SNA session information (such as line and PU status) obtained by VTAM for each session, and the IP address of the remote host connected to the session.

To display the Enterprise Extender Session List, do this:

1. Enter **SL** (Session List) beside an EE entry on the IP resource monitor (/IPMON). The Session List is displayed.

```
PROD-------------------- TCP/IP : Session List --------------------------------
Command ===>                                                 Function=Update

. Session List Command Filter Input Fields ----------------------------------.
|                                                                             |
|  Line .................                  (Optional)                       |
|  Line Status ..........                  (Optional)                       |
|  IP Address ...........                  (Optional)                       |
|                                                                             |
.-----------------------------------------------------------------------------.
```

2. Type values in any of the Session List Command Filter Input Fields that you require.

3. Press F6 (Action). The Enterprise Extender Session List is displayed.

```
PROD------------ TCP/IP : Enterprise Extender Session List -------------------
Command ===>                                                 Scroll ===> PAGE

    Line      Line Status  Line Type  PU        PU Status   Remote IP Address
    EE01L000  ACTIV        DIAL-IN
    EE01L001  ACTIV        DIAL-IN    CN000029  ACTIV---X-  10.112.4.253
    EE01L002  ACTIV        DIAL-IN
    EE01L003  ACTIV        DIAL-IN
    EE01L004  ACTIV        DIAL-IN
    EE01L005  ACTIV        DIAL-IN
    EE01L006  ACTIV        DIAL-IN
    EE01L007  ACTIV        DIAL-IN
    EE01L008  ACTIV        DIAL-IN    CN000039  ACTIV---X-  10.112.4.85
    EE01L009  ACTIV        DIAL-IN    CN00002C  ACTIV---X-  10.112.4.93
    **END**
```

For details of the information displayed, press F1 (Help).

Displaying UDP Port Activity

The Enterprise Extender UDP Port Activity panel displays UDP port information regarding the data flows over the identified UDP ports.

To display the Enterprise Extender UDP Port Activity panel, enter **UA** (UDP Port Activity) beside an EE entry on the IP resource monitor (/IPMON).

To display the Enterprise Extender UDP Port Activity panel, do this:

1. Enter **UA** (UDP Port Activity) beside an EE entry on the IP resource monitor (/IPMON). The UDP Port Activity panel is displayed.

```
PROD------------------- TCP/IP : UDP Port Activity ----------------------------
Command ===>                                                 Function=Update

. UDP Port Activity Command Input Field ---------------------------------------.
|                                                                              |
|  First Port Number ....              (Optional)                              |
|                                                                              |
|  Note                                                                        |
|  Leave this field blank unless the system administrator has allocated        |
|  a non-standard port range. (The standard port range is 12000 to 12004.)     |
|                                                                              |
.------------------------------------------------------------------------------.
```

2. Type a value in the First Port Number fields if you require it.

3. Press F6 (Action). The Enterprise Extender UDP Port Activity panel is displayed.

```
PROD---------- TCP/IP : Enterprise Extender UDP Port Activity -----------------
Command ===>                                                  Scroll ===> PAGE

                 Idle     ------Bytes------ ----Datagrams---- ----Maximum----
   Port  Type    Time          In      Out       In      Out       In     Out
   12000 Signal  00:00:01   65.74K   66.18K   5.829K   5.826K  65.54K  65.54K
   12001 Network 00:00:00   1.340M   1.183M   21.03K   20.97K  65.54K  65.54K
   12002 High    05:42:54        0        0        0        0  65.54K  65.54K
   12003 Medium  00:00:00   476.8K   652.2K   7.266K   7.240K  65.54K  65.54K
   12004 Low     05:42:54        0        0        0        0  65.54K  65.54K
   **END**
```

For details of the information displayed, press F1 (Help).

Monitoring Enterprise Extender Performance

The Monitor Enterprise Extender Performance panel displays collected performance data and provides graphs of selected communication attributes. You can monitor the following areas of Enterprise Extender communications to ensure their services are available:

- Traffic through Enterprise Extender ports
- Availability of SNA lines to satisfy new connection requests

To display the Monitor Enterprise Extender Performance panel, enter **H** (History) beside an EE resource on the IP resource monitor (/IPMON).

```
PROD------------ TCP/IP : Monitor Enterprise Extender Performance -------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... EE
     Description ......... EE Monitoring Definition
     Current Alerts ...... 2
                                        E=Expand C=Contract  S/=Summary D=Detail
                                  - Alerts --          Last
    Attribute/Qualifier          Open  Total Samples Sample        Value Type
     |-- Lines                                0      51 13:55            - GAUGE
     | |-- LinesActive                        0      17 13:55           10 GAUGE
     | |-- LinesFree                          0      17 13:55           10 GAUGE
     | |-- LineTotal                          0      17 13:55           10 GAUGE
     |-- Byte count                           0      85 13:55            - COUNT
       |-- HighPriorityData                   0      17 13:55            0 COUNT
       |-- LowPriorityData                    0      17 13:55            0 COUNT
       |-- MediumPriorityData                 0      17 13:55            0 COUNT
       |-- NetworkPriorityData                0      17 13:55            0 COUNT
       |-- SignalTraffic                      0      17 13:55         9504 COUNT
    **END**
 F1=Help      F2=Split     F3=Exit      F4=Expand    F5=Find      F6=AutoRfsh
 F7=Backward  F8=Forward   F9=Swap                  F11=Right    F12=ByAttr
```

For details of the information displayed and the actions available on the Monitor Enterprise Extender Performance panel, press F1 (Help).

Chapter

12

Monitoring CSM Resources

This chapter contains the following topics:

- Monitoring Your CSM Resources
- Displaying CSM Usage
- Monitoring CSM Performance

Monitoring Your CSM Resources

The CSM (Communications Storage Manager), a component of the OS/390 Communications Server, is used by authorized host applications to manage subsystem storage pools and to allow CSM users to share data without having to physically move the data.

You can use the IP resource monitor to display information about your CSM resources.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources ------------------------
Command ===>                                                  Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                          Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual  Status   Count  Sev  Samp  Samp
    QANM         ASMON    QANM18   ACTIVE  Ok       0      0    16:17 17:17
    CIPQA18      CIP      QANM18   ACTIVE  Ok       0      0    16:17 17:17
    CSM          CSM      QANM18   ACTIVE  Ok       4      2    16:17 17:17
    EE           EE       QANM18   ACTIVE  Ok       0      0    16:37 16:47
    OSADEX       OSA      QANM18   ACTIVE  Ok       0      0    16:26 17:26
    OSAEX        OSA      QANM18   ACTIVE  Ok       0      0    16:26 17:26
    QAS2         OSA      QANM18   ACTIVE  Ok       0      0    16:26 17:26
    ROTQ18       ROUTER   QANM18   ACTIVE  Ok       0      0    16:17 17:17
    TCPICSD1     STACK    QANM18   ACTIVE  Ok       0      0    16:17 17:17
    TCPIP38      STACK    QANM18   ACTIVE  Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

IP Resource Commands

To view the commands available for a CSM resource, enter **?** next to a CSM entry.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to CSM resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** next to it.

CSM Resource Commands

The commands specific to CSM resources are:

Command	Description
AL	View alerts for a resource
ALH	View alerts history for a resource
AM	Activate monitoring
D	Display CSM usage
H	Show performance history
IM	Inactivate monitoring
UM	Update resource monitoring definition

Displaying CSM Usage

The CSM Usage by Buffer panel (or the CSM Usage by Job panel) provides information about the buffer usage of the CSM from the perspective of the selected NetMaster region.

To display the CSM Usage by Buffer (or by Job) panel, enter **D** (Display CSM Usage) next to a CSM entry on the IP resource monitor (/IPMON).

```
PROD------------------- TCP/IP : CSM Usage by Buffer -------------------------
Command ===>                                                 Scroll ===> PAGE

Fixed maximum .............   120M       ECSA maximum ............. 75542K
Fixed current .............  1420K       ECSA current .............  1243K
Fixed maximum used ........  1420K       ECSA maximum used ........  1243K
Fixed recommended value ...  2130K       ECSA recommended value ...  1865K

    Buffer size  Buffer source  Jobname    In use     Free    Total
             4K  ECSA           (all)         60K     260K     320K
                                VTAM          40K
                                TCPIPC        20K
            16K  ECSA           (all)          0      256K     256K
            32K  ECSA           (all)          0      512K     512K
            60K  ECSA           (all)          0         0        0
           180K  ECSA           (all)          0         0        0
          Total  ECSA           (all)         60K    1028K    1088K
                                VTAM          40K
                                TCPIPC        20K
             4K  Data Space     (all)        316K     196K     512K
                                VTAM         304K
                                TCPIPC        12K
            16K  Data Space     (all)          0      256K     256K
            32K  Data Space     (all)          0      512K     512K
            60K  Data Space     (all)          0         0        0
           180K  Data Space     (all)          0     1800K    1800K
          Total  Data Space     (all)        316K    2764K    3080K
                                VTAM         304K
                                TCPIPC        12K
          Total  All Sources    (all)        376K    3792K    4168K
                                VTAM         344K
                                TCPIPC        32K
    **END**
```

For details of the information displayed and actions available, press F1 (Help).

Use F4 to toggle between displays of usage by job and by buffer.

Monitoring CSM Performance

The CSM performance panel displays collected performance data and graphs of selected CSM attributes. You can view the total usage of CSM storage and the amount used by individual applications.

To display the Monitor CSM Performance panel, enter **H** (Show Performance History) next to a CSM entry on the IP resource monitor (/IPMON).

```
PROD----------------- TCP/IP : Monitor CSM Performance ------------------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... CSM
     Description ......... CSM Monitoring Definition
     Current Alerts ...... 4
                                        E=Expand C=Contract  S/=Summary D=Detail
                                 - Alerts --          Last
    Attribute/Qualifier          Open  Total Samples Sample        Value Type
     |-- (all)                      2      4      20 15:07            - GAUGE
     |-- TCPIP38                    1      2       8 15:07            - GAUGE
     |-- VTAM                       1      2       8 15:07            - GAUGE
    **END**
```

For details of the information displayed and actions available, press F1 (Help).

Chapter 13

Monitoring Address Spaces

This chapter contains the following topics:

- Monitoring Your Address Spaces
- Monitoring Address Space Performance

Monitoring Your Address Spaces

You can use the IP resource monitor to display information about your address spaces, which are shown as class ASMON.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources ------------------------
Command ===>                                                 Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                                Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual      Status   Count  Sev  Samp  Samp
    QANM         ASMON    QANM18   ACTIVE      Ok       0      0    16:17 17:17
    CIPQA18      CIP      QANM18   ACTIVE      Ok       0      0    16:17 17:17
    CSM          CSM      QANM18   ACTIVE      Ok       4      2    16:17 17:17
    EE           EE       QANM18   ACTIVE      Ok       0      0    16:37 16:47
    OSADEX       OSA      QANM18   ACTIVE      Ok       0      0    16:26 17:26
    OSAEX        OSA      QANM18   ACTIVE      Ok       0      0    16:26 17:26
    QAS2         OSA      QANM18   ACTIVE      Ok       0      0    16:26 17:26
    ROTQ18       ROUTER   QANM18   ACTIVE      Ok       0      0    16:17 17:17
    TCPICSD1     STACK    QANM18   ACTIVE      Ok       0      0    16:17 17:17
    TCPIP38      STACK    QANM18   ACTIVE      Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

IP Resource Commands

To view the commands available for an address space, enter **?** next to an ASMON entry.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to address spaces come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** next to it.

Address Space Commands

The commands specific to address spaces are:

Command	Description
AL	View alerts for a resource
ALH	View alerts history for a resource
AM	Activate monitoring
D	Display resource status
H	Show performance history
IM	Inactivate monitoring
UM	Update resource monitoring definition

Monitoring Address Space Performance

The Monitor Address Space Performance panel displays collected performance data and graphs of selected address space attributes. You can view address space attributes to ensure their services are available.

To display the Monitor Address Space Performance panel, enter **H** (Show Performance History) next to an ASMON entry on the IP resource monitor (/IPMON).

```
PROD------------ TCP/IP : Monitor Address Space Performance -------------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... CSM
     Description ......... CSM Monitoring Definition
     Current Alerts ...... 4
                                      E=Expand C=Contract  S/=Summary D=Detail
                                - Alerts --          Last
    Attribute/Qualifier          Open  Total Samples Sample        Value Type
     |-- (all)                      2      4      20 15:07            - GAUGE
     |-- TCPIP38                    1      2       8 15:07            - GAUGE
     |-- VTAM                       1      2       8 15:07            - GAUGE
    **END**
```

For details of the information displayed and actions available, press F1 (Help).

Chapter

14

Monitoring CICS Resources

This chapter contains the following topics:

- Monitoring Your CICS Resources
- Listing CICS Connections from a Socket Management Perspective
- Displaying Information About a CICMON Resource
- Shutting Down and Restarting Socket Management for CICS and CPT
- Stopping and Restarting the Command Server Interface
- Starting a CICS Server
- Starting CICS Transactions
- Monitoring CICS Resource Performance

Monitoring Your CICS Resources

If NetMaster Socket Management for CICS is configured in your region, you can use the IP resource monitor to display information about your CICS Socket Management resources, which are shown as class CICMON.

See *Unicenter NetMaster Socket Management for CICS Getting Started* for information about NetMaster Socket Management for CICS.

To access the IP resource monitor, enter **/IPMON** at the ===> prompt.

```
PROD------------------- Status Monitor : IP Resources -------------------------
Command ===>                                                  Scroll ===> PAGE

                              S=Status L=Log H=History DB=Database ?=List Cmds
                                          Monitor  Alert  Max  Last  Next
    Resource     Class    System   Actual  Status   Count  Sev  Samp  Samp
    QANM         ASMON    QANM18   ACTIVE  Ok       0      0    16:17 17:17
    CIPQA18      CIP      QANM18   ACTIVE  Ok       0      0    16:17 17:17
    CSM          CSM      QANM18   ACTIVE  Ok       4      2    16:17 17:17
    EE           EE       QANM18   ACTIVE  Ok       0      0    16:37 16:47
    OSADEX       OSA      QANM18   ACTIVE  Ok       0      0    16:26 17:26
    OSAEX        OSA      QANM18   ACTIVE  Ok       0      0    16:26 17:26
    QAS2         OSA      QANM18   ACTIVE  Ok       0      0    16:26 17:26
    ROTQ18       ROUTER   QANM18   ACTIVE  Ok       0      0    16:17 17:17
    QATS13D3     CICMON   NMDD     ACTIVE  Ok       0      0    16:17 17:17
    TCPICSD1     STACK    QANM18   ACTIVE  Ok       0      0    16:17 17:17
    TCPIP38      STACK    QANM18   ACTIVE  Ok       0      0    16:17 17:17
    **END**
```

For details of the information displayed, press F1 (Help).

IP Resource Commands

To view the commands available for a CICS resource, enter **?** next to a CICMON resource.

A panel is displayed, listing the available commands in alphanumeric order by name in two groups. Commands that are specific to CICS resources come first (displayed in turquoise), followed by other relevant commands. To execute a command, enter **S** next to it.

CICS Resource Commands

The commands specific to CICS resources are:

Command	Description
AL	View alerts for a resource
ALH	View alerts history for a resource
AM	Activate monitoring
CL	Connections list via SocketMgmt
CMD	Command entry - SocketMgmt
D	Display resource status
DUI	Delete SocketMgmt user info for server
H	Show performance history
IC	IP connections
ICC	IP CICS connections
IM	Inactivate monitoring
SB	SocketMgmt and CPT bounce
SQ	SocketMgmt query display
SS	CICS server start
SSB	SocketMgmt CMD server bounce
TS	CICS transaction start
UM	Update resource monitoring definition
W	Display outstanding WTORs for JOB/STC

Listing CICS Connections from a Socket Management Perspective

To list CICS connections from a Socket Management perspective, enter **CL** (Connections List via SocketMgmt) next to a CICMON resource on the IP resource monitor (/IPMON).

```
PROD------------------- SocketMgmt : Connections List -------------------------
Command ===>                                                 Scroll ===> PAGE

        CICS Jobname ..... CICSPRDA
                                    S/DC=Display Connection ZC=Drop Connection

               Local  Remote  Remote           Connection  CICS
    SMID        Port    Port  Address          Type        Terminal   User ID
    3           2257       *  *                LISTENER    -          JCH3
    5           1846       *  *                LISTENER    -          JCH3
    89          2257   20051  123.123.123.45   INBOUND     -          JCH3
    101         2257   20064  123.123.123.45   INBOUND     -          JCH3
    **END**
```

For details of the information displayed and actions available, press F1 (Help).

Displaying Information About a CICMON Resource

To display information about a CICMON resource, enter **SQ** (SocketMgmt Query Display) next to a CICMON resource on the IP resource monitor (/IPMON).

```
PROD---------------------- SocketMgmt : Information --------Columns 00001 00079
Command ===>                                                 Scroll ===> PAGE

 SocketMgmt and CPT Summary
   CICS Jobname ............. - QATS13D3
   TCP/IP Jobname ........... - WTMCC600
          SSID .............. - WTM1
          Trace SSID ........ - WTMV
   CMD Server Address ....... - 123.123.123.123
   CMD Server Port .......... - 2257

   Running Products ......... - +CPT+SOCKETMGMT
   SocketMgmt Release ....... - 1.0.0
   CPT Release .............. - 6.0.0
   Startup Config Member .... - T09CONFG
   Security Exit Name ....... - -

Connection Summary
   Bytes Received ........... - 4332
   Bytes Sent ............... - 9918
   Calls Received ........... - 94
   Calls Sent ............... - 74
****************************** BOTTOM OF DATA ******************************
```

For details of the information displayed and actions available, press F1 (Help).

Shutting Down and Restarting Socket Management for CICS and CPT

To shut down and restart Socket Management for CICS and CPT inside the CICS environment:

1. Enter **SB** (SocketMgmt and CPT Bounce) next to a CICMON resource on the IP resource monitor (/IPMON). A confirmation panel is displayed.

```
PROD-------------------- SocketMgmt : Bounce Confirmation ---------------------
Command ===>

 _ SocketMgmt and CPT Bounce Command ____________________________________________
|                                                                               |
|     WARNING: This command will stop and restart Socket Management and CPT     |
|                                                                               |
|     T09CONxx Startup Config Member Suffix __   (default is current suffix)    |
|                                                                               |
|  SocketMgmt and CPT Summary:                                                  |
|     CICS Jobname ....................... QATS13D3                            |
|     TCP/IP Jobname ..................... WTMCC600                            |
|     Running Products ................... +CPT+SOCKETMGMT                     |
|     Startup Config Member .............. T09CONFG                            |
|                                                                               |
 _______________________________________________________________________________

  Press the Confirm key to confirm the request or the Cancel key to cancel.


 F1=Help      F2=Split                                          F6=Confirm
                           F9=Swap                            F12=Cancel
```

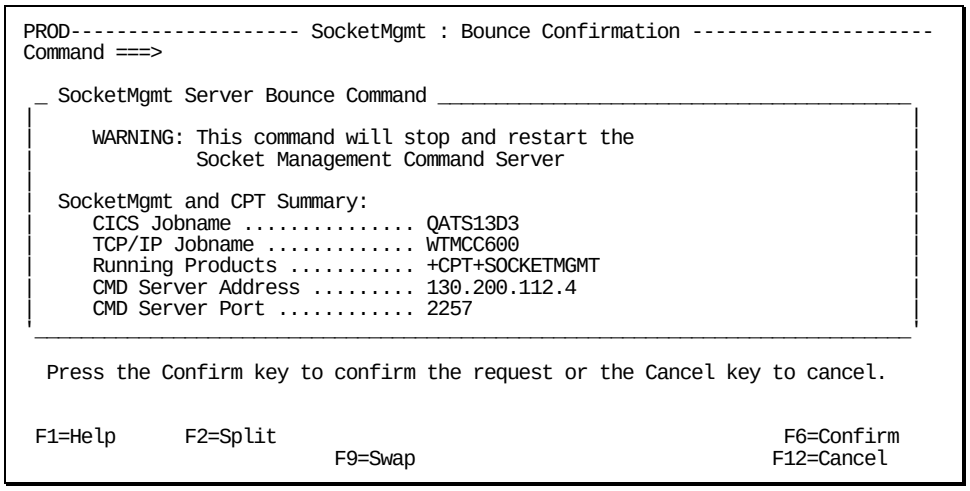
2. Type a value in the T09CON*xx* Startup Config Member Suffix field (or leave it blank for the default value).
3. Press F6 (Confirm) to confirm the request. The following message is displayed:

```
RMCALL25 'SB' COMMAND PROCESSING COMPLETE
```

Stopping and Restarting the Command Server Interface

To stop and restart the Socket Management for CICS command server interface:

1. Enter **SSB** (SocketMgmt CMD Server Bounce) next to a CICMON resource on the IP resource monitor (/IPMON). A confirmation panel is displayed.



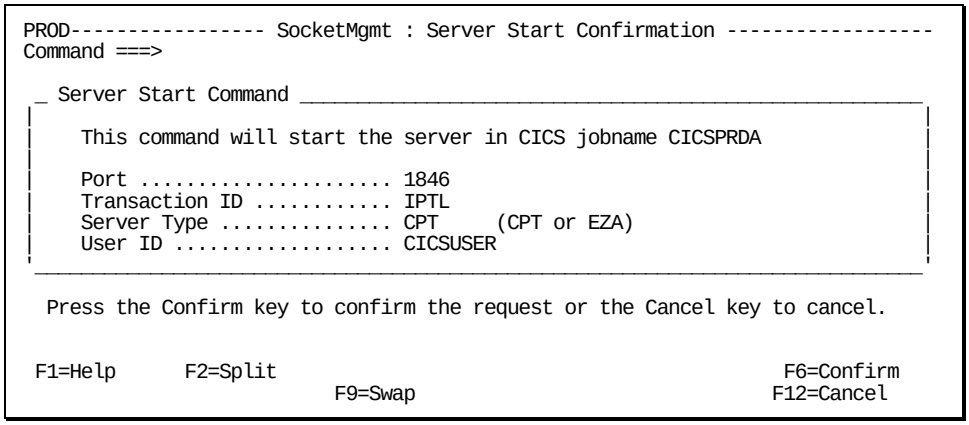
2. Press F6 (Confirm) to confirm the request. The following message is displayed:

```
RMCALL25 'SSB' COMMAND PROCESSING COMPLETE
```

Starting a CICS Server

To start a CICS server:

1. Enter **SS** (CICS Server Start) next to a CICMON resource on the IP resource monitor (/IPMON). A confirmation panel is displayed, where you must enter parameters for the server.

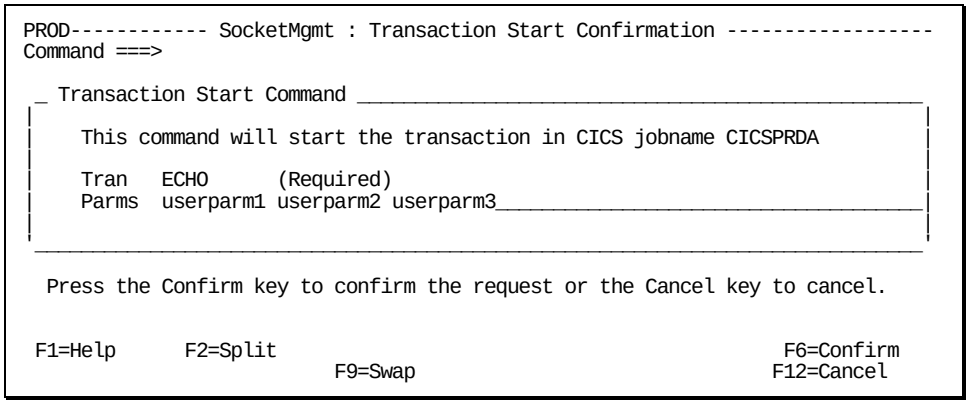


2. Type values in the fields required (only Port is mandatory).
3. Press F6 (Confirm) to confirm the request.
4. The CICS server is started.

Starting CICS Transactions

To start a CICS transaction in a CICS environment:

1. Enter **TS** (CICS Transaction Start) next to a CICMON resource on the IP resource monitor (/IPMON). A confirmation panel is displayed, where you can enter parameters for the transaction.



5. Type a value in the Tran field.
6. In the Parms field, type the names of any parameters that you wish to supply to the CICS transaction.
7. Press F6 (Confirm) to confirm the request.
8. The CICS transaction is started.

Monitoring CICS Resource Performance

The Monitor CICS Performance panel displays collected performance data and graphs of selected CICS attributes. You can view CICS attributes to ensure their services are available.

To display the Monitor CICS Performance panel, enter **H** (Show Performance History) next to a CICMON resource on the IP resource monitor (/IPMON).

```
PROD----------------- TCP/IP : Monitor CICS Performance -----------------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... CICS
     Description ......... CICS Monitoring Definition
     Current Alerts ...... 4
                                        E=Expand C=Contract  S/=Summary D=Detail
                                - Alerts --          Last
    Attribute/Qualifier          Open  Total Samples Sample        Value Type
     |-- TESTCICS                          0      78 17:22            - -
       |-- CPU%                            0      13 17:22         0.00 GAUGE
       |-- EXCP                            0      13 17:22            0 GAUGE
       |-- JobCount                        0      13 17:22            0 GAUGE
       |-- SRBCPU                          0      13 17:22            0 GAUGE
       |-- TaskCPU                         0      13 17:22            0 GAUGE
       |-- TotalCPU                        0      13 17:22            0 GAUGE
    **END**
```

For details of the information displayed and actions available, press F1 (Help).

Chapter

15

Monitoring Alerts and IP Nodes

This chapter contains the following topics:

- Monitoring Active Alerts
- Working with Alerts
- Raising Trouble Tickets for Alerts
- Displaying Alert Details
- Displaying Alert History
- Monitoring IP Nodes

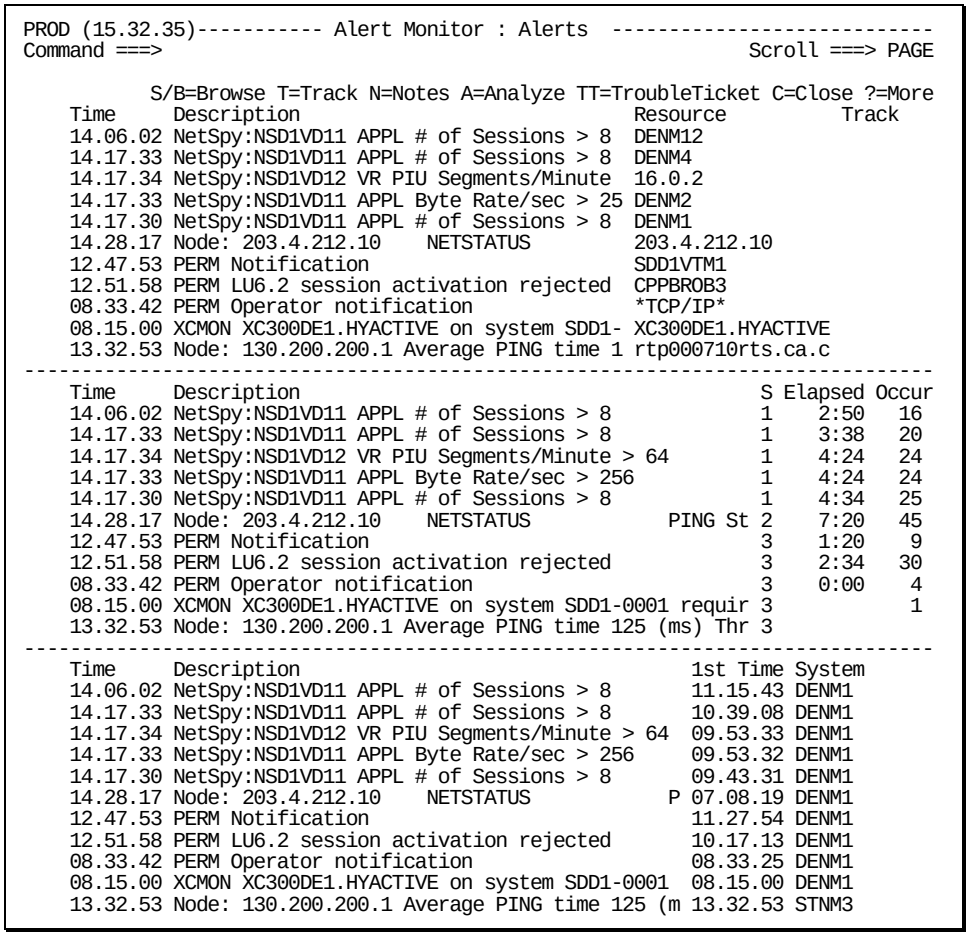
Monitoring Active Alerts

The Alert Monitor provides an integrated, correlated event notification system that indicates to network operators that a problem has been detected and that some action needs to be taken. Such alerts from NetMaster for TCP/IP, known as active alerts, are displayed on the alert monitor. Alerts that were raised before the system was shut down are not displayed on the Alert Monitor panel when the system is restarted, but are displayed on the Alert History panel. The alert history contains information about alerts that are no longer active (closed alerts).

The alert monitor can initiate actions such as starting recovery procedures, and creating trouble tickets, either automatically or manually.

For information about both active and closed alerts, see the section “Displaying Alert History”.

To display alerts on the Alert Monitor, enter **/ALERTS** at the ===> prompt.



```
PROD (15.32.35)----------- Alert Monitor : Alerts  ---------------------------
Command ===>                                                 Scroll ===> PAGE

          S/B=Browse T=Track N=Notes A=Analyze TT=TroubleTicket C=Close ?=More
    Time     Description                              Resource          Track
    14.06.02 NetSpy:NSD1VD11 APPL # of Sessions > 8  DENM12
    14.17.33 NetSpy:NSD1VD11 APPL # of Sessions > 8  DENM4
    14.17.34 NetSpy:NSD1VD12 VR PIU Segments/Minute  16.0.2
    14.17.33 NetSpy:NSD1VD11 APPL Byte Rate/sec > 25 DENM2
    14.17.30 NetSpy:NSD1VD11 APPL # of Sessions > 8  DENM1
    14.28.17 Node: 203.4.212.10    NETSTATUS         203.4.212.10
    12.47.53 PERM Notification                       SDD1VTM1
    12.51.58 PERM LU6.2 session activation rejected  CPPBROB3
    08.33.42 PERM Operator notification              *TCP/IP*
    08.15.00 XCMON XC300DE1.HYACTIVE on system SDD1- XC300DE1.HYACTIVE
    13.32.53 Node: 130.200.200.1 Average PING time 1 rtp000710rts.ca.c
-------------------------------------------------------------------------------
    Time     Description                                        S Elapsed Occur
    14.06.02 NetSpy:NSD1VD11 APPL # of Sessions > 8             1    2:50   16
    14.17.33 NetSpy:NSD1VD11 APPL # of Sessions > 8             1    3:38   20
    14.17.34 NetSpy:NSD1VD12 VR PIU Segments/Minute > 64        1    4:24   24
    14.17.33 NetSpy:NSD1VD11 APPL Byte Rate/sec > 256           1    4:24   24
    14.17.30 NetSpy:NSD1VD11 APPL # of Sessions > 8             1    4:34   25
    14.28.17 Node: 203.4.212.10    NETSTATUS            PING St 2    7:20   45
    12.47.53 PERM Notification                                  3    1:20    9
    12.51.58 PERM LU6.2 session activation rejected             3    2:34   30
    08.33.42 PERM Operator notification                         3    0:00    4
    08.15.00 XCMON XC300DE1.HYACTIVE on system SDD1-0001 requir 3            1
    13.32.53 Node: 130.200.200.1 Average PING time 125 (ms) Thr 3
-------------------------------------------------------------------------------
    Time     Description                                   1st Time System
    14.06.02 NetSpy:NSD1VD11 APPL # of Sessions > 8       11.15.43 DENM1
    14.17.33 NetSpy:NSD1VD11 APPL # of Sessions > 8       10.39.08 DENM1
    14.17.34 NetSpy:NSD1VD12 VR PIU Segments/Minute > 64  09.53.33 DENM1
    14.17.33 NetSpy:NSD1VD11 APPL Byte Rate/sec > 256     09.53.32 DENM1
    14.17.30 NetSpy:NSD1VD11 APPL # of Sessions > 8       09.43.31 DENM1
    14.28.17 Node: 203.4.212.10    NETSTATUS            P 07.08.19 DENM1
    12.47.53 PERM Notification                            11.27.54 DENM1
    12.51.58 PERM LU6.2 session activation rejected       10.17.13 DENM1
    08.33.42 PERM Operator notification                   08.33.25 DENM1
    08.15.00 XCMON XC300DE1.HYACTIVE on system SDD1-0001  08.15.00 DENM1
    13.32.53 Node: 130.200.200.1 Average PING time 125 (m 13.32.53 STNM3
```

By default, alerts are sorted in order of highest severity, then in date and time order. This is equivalent to issuing the SORT command:

SORT S ASCENDING, DATE DESCENDING, TIME DESCENDING

You can change the sort order by using the SORT command. You can locate an alert by the sorted fields by using the LOCATE command.

For details of the syntax of the SORT command, enter **SORT ?** at the ===> prompt.

For details of the information displayed and the actions available, press F1 (Help).

Commands on the Alert Monitor Panel

You can issue the following commands at the ===> prompt:

- SORT
- LOCATE
- FILTER
- DEFINE FILTER
- FORMAT
- DEFINE FORMAT
- HISTORY

For information about these commands, press F1 (Help) from the Alert Monitor panel.

Working with Alerts

The alert monitor displays the alert when it arrives. Alerts can be closed automatically by NetMaster for TCP/IP or manually by the operator. When an alert is closed, it is removed from the active alert monitor. However, it is still accessible from the Alert History panel.

Typically, when an alert arrives, do this:

1. Browse the alert to find out whether any suggested recommended actions are provided. To browse the alert, enter **B** beside the alert.
2. To respond to an alert, indicate to other users that you will be working on it. To do this, enter **T** beside the alert. Your user ID is displayed in the Track column.
3. Perform any necessary actions to remove the alert condition. (For information about actions, press F1 (Help).)
4. Record notes that provide future reference information about this alert in the alert definition. To do this, enter **N** beside the alert.
5. After the alert condition is resolved, close the alert (if required). To do this, enter **C** beside the alert.

Raising Trouble Tickets for Alerts

Your site is likely to have site-specific procedures for raising trouble tickets. Depending on your site-specific setup, you can send a trouble ticket in the form of an e-mail or by using a customized NCL procedure. (For information about customized procedures at your site, see your System Administrator.)

To use the procedure defined at your site for raising a trouble ticket, apply the **TT**=TroubleTicket action at the Alert Monitor panel.

The Trouble Ticket action produces a request for a trouble ticket as defined to your NetMaster system.

Displaying Alert Details

The Alert Display panel describes an active alert, and provides information about its generation time and its identity. An alert comes with the following information:

- General information such as severity level, the source of the alert, and update history
- Possible causes of the alert and any recommended actions

To display the Alert Display panel, enter **B** or **S** beside an alert at the Alert Monitor panel (/ALERTS).

```
PROD---------------- Alert Monitor : Alert Display ---------Columns 00001 00079
Command ===>                                                 Scroll ===> CSR

Alert Description
 Node: 11.22.33.44     NETSTATUS            PING Status: Timeout

Alert History
 Created at .................. FRI 31-AUG-2001  07.51.15
 Last Updated at ............. FRI 31-AUG-2001  07.51.15
 Number of occurrences ....... 18
 Elapsed time ................ 2 hours 50 minutes
 Last occurred at ............ FRI 31-AUG-2001  10.41.14

Alert Identification
 Severity ............ 2 (High)

 System .............. PROD

 Application ......... TCP/IP Services

 Alert Class ......... IPMONVALUE
 Class Description ... IP Node Monitor Attribute Status

 Resource ............ 11.22.33.44

Alert Explanation
 The alert contains variable data that is identified by the
 characters Pn (where n is a number) in the following:
    Node: P1 PING Status: P2

 An alert has been created by the IP Node Monitor function.
 The monitor attempted to ping the node with IP address P1
  P2 is the status detected, it may be one of:
   Timeout - The ping request for device timed out.
   Unknown - Either a ping has not yet been done or the TCP/IP Services
             interface is unavailable.

System Action
 An alert is created.

Recommended Action
 Check the status of the resource, possibly by issuing the CH=CHECK
 action against the node in the IP Node Monitor.
```

For details of the information displayed, press F1 (Help).

Printing Alert Details

To print details of the displayed alert, enter **PRINT** at the ===> prompt.

Displaying Alert History

The alert history lists all alerts, both active and closed, that occurred on the local region during a period.

To view the alert history from the Alert Monitor panel, press F4 (History). The alerts for the current date are displayed. To display the alerts for other dates, use the DATE command. (For information about the DATE command, press F1 (Help).)

Note: History records are retained only for a certain number of days. To define or change history logging parameters, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide*.

For details of the information displayed and actions available, press F1 (Help).

Commands on the Alert History Panel

You can issue the following commands at the ===> prompt:

- SORT
- LOCATE
- DATE

For information about these commands, press F1 (Help) from the Alert History panel.

Monitoring IP Nodes

The IP node monitor facility allows you to monitor important IP nodes on a regular basis. It also allows you to define alerts to be displayed on the alert monitor by using a defined policy (for example, if the IP node is unreachable or if its round trip time is outside certain limits). (For information about alerts, see the section “Monitoring Active Alerts”.)

A host name or IP address is specified for monitoring. The resolved address is then polled at regular intervals for the values you are interested in. Usually this includes a ping. If the ping is successful, the displayed device status indicates the device is reachable; if the ping is unsuccessful, the displayed device status indicates it is unreachable.

A change in state is advertised by an Event Distribution Services (EDS) event. For further information about EDS events, see the appendix “Enhanced Automation” in the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide.*

To monitor IP nodes, enter /IPNODE at a ===> prompt. The TCP/IP : IP Node Monitor is displayed.

```
PROD--------------------- TCP/IP : IP Node Monitor ----------------------------
Command ===>                                                  Scroll ===> CSR

              P=Ping T=TraceRoute S=System Info I=Interfaces TN=Telnet CH=Check
                     A=Alerts H=History U=Update D=Delete R=Routing Table
                                                    .-- Last Ping --.  Next
     IP Address      Host Name                Status   Avg   Max   Time    Samp
     123.168.11.33   abcCIP-Telnet2           OK       24    41    14:10  14:10
     123.0.88.22     abcmvs1.abc.col          OK       7     15    14:15  14:30
     123.0.80.26                              Unknown  -     -     -
     123.0.80.30     -                        OK       29    49    14:10  14:10
     123.0.81.1      -                        OK       28    44    14:05  14:05
     123.0.88.55     xyzprod.abc.col          OK       22    25    14:10  14:10
     123.0.90.1      frodo.abc.co             OK       504   559   14:05  14:05
-------------------------------------------------------------------------------
                     .---- Ping Averages By Period ---. .-- Alert --.
     IP Address      Hour   -1     -2     -3     24hr   RTT   Timeout
     123.168.11.33   18     -      26     132    54     -      -
     123.0.88.22     7      -      7      166    58     -      -
     123.0.80.26     -      -      -      -      -      -      -
     123.0.80.30     33     -      65     285    120    -      -
     123.0.81.1      60     -      28     239    98     -      -
     123.0.88.55     42     -      32     315    120    -      -
     123.0.90.1      585    -      517    1374   729    -      -
-------------------------------------------------------------------------------
     IP Address      Monitor Group
     123.168.11.33   CISCOMONINTENS
     123.0.88.22     192.000.080.025
     123.0.80.26     CISCOPERFINTENS
     123.0.80.30     CISCOMONINTENS
     123.0.81.1      192.000.081.001
     123.0.88.55     CISCOMONINTENS
     123.0.90.1      192.000.090.001
```

For details of the information and actions available, press F1 (help).

Filtering IP Nodes

The FILTER command allows you to display a subset of IP nodes being monitored. You can select the display of a subset of IP nodes based on the following attributes:

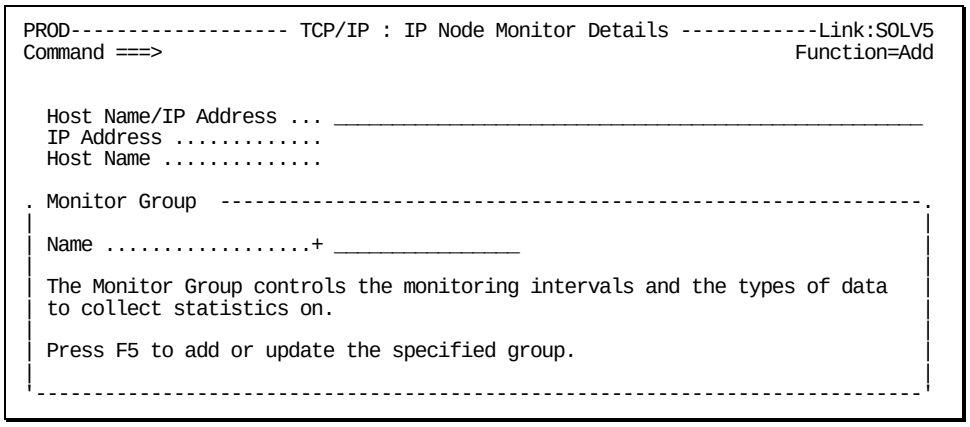
- IP address
- Status
- Group name

For further details, press F1 (help).

Adding an IP Node to Be Monitored

To add another IP node to be monitored by the IP node monitor:

1. Press F4 (Add) on the IP node monitor (/IPNODE). The IP Node Monitor Details panel is displayed.



2. In the Host Name/IP Address field, enter the host name, or IP address, of the IP node that you want to add to the IP Node Monitor.
3. Enter the name of the Monitor Group (or enter **?** to display a selection list of monitor groups).

   Note: By pressing F5 to display the IP Node Monitor Group Details, you can update the monitor group with changes to the monitoring intervals and types of data to collect. Any change you make to the monitor group will apply to all resources belonging to that group.
4. Press F4 (Save). You are returned to the IP node monitor.

Fields and Actions on the IP Node Monitor Details Panel

For information about the input fields and actions available, press F1 (Help).

Chapter

16

Diagnosing Printer Problems

This chapter contains the following topic:

- Determining Printer Problems

Determining Printer Problems

The line printer diagnostics allow you to determine if there are printer problems on the network by displaying a print queue or by issuing a test print to a remote line printer (LP) server. You can also delete an item from the print queue, if necessary.

To access the line printer diagnostics, enter **/LPD** at a ===> prompt.

```
PROD---------------- TCP/IP : Line Printer (LPD) Diagnostics -------------/LPD
Select Option ===>

   Q   - Query Print Queue
   D   - Delete a Job from the Print Queue
   PR  - Send a Test Print to a Printer
   X   - Exit

Host Name/Addr ..                                        ( Required ALL )
Printer Name ....                                        ( Required ALL )
Job Number ......                                        ( Required D )
User Name ....... USER01                                 ( Required D )
Link Name ......+                                        ( Optional ALL )
```

For information about the input fields, press F1 (Help).

Querying Printer Status

To display a printer queue, do this:

1. At the TCP/IP : Line Printer (LPD) Diagnostics Menu, type **Q** at the ===> prompt.
2. Complete any required fields on the panel.
3. Press ENTER.

The printer status panel is displayed. The contents of this panel depend on the remote LPD implementation.

If your region receives an error return code instead of the printer status display, it automatically pings the IP address of the printer's host to determine the cause of the failure. If the ping is successful, it proves that the host is contactable but that the printer is not, or that the printer daemon resident in the host is not active.

```
PROD--------------------- TCP/IP : Browse Print Queue ----------Columns 001 079
Command ===>                                                   Scroll ===> CSR

IP Host Name/Address .... 199.0.90.189
Printer Name ............ printer01

******************************** TOP OF DATA *********************************
                        Windows NT LPD Server
                             Printer printer01

Owner       Status         Jobname          Job-Id    Size   Pages  Priority
-------------------------------------------------------------------------------
USER01 (199 Paused    PROD1.USER01.DOC/DE      3       401      0      1
USER01 (199 Paused    PROD1.USER01.DOC/MA      5      3945      0      1
USER01 (199 Paused    PROD1.USER01.DOC/MA      7       749      0      1
USER01 (199 Paused    PROD1.USER01.DOC/NE      9      1595      0      1
USER01 (199 Paused    PROD1.USER01.DOC/NM     11      1985      0      1
USER01 (199 Paused    PROD1.USER01.DOC/PU     13       624      0      1
USER01 (199 Paused    PROD1.USER01.DOC/DE     15       401      0      1
USER01 (199 Paused    PROD1.USER01.DOC/MA     17      3945      0      1
USER01 (199 Paused    PROD1.USER01.DOC/MA     19       749      0      1
USER01 (199 Paused    PROD1.USER01.DOC/NE     21      1595      0      1
 F1=Help      F2=Split     F3=Exit                  F5=Find
 F7=Backward  F8=Forward   F9=Swap     F10=Left     F11=Right
```

Deleting an Entry in the Print Queue

To delete a job from the print queue, do this:

1. At the TCP / IP : Line Printer (LPD) Diagnostics Menu, select option **D** - Delete a Job from the Print Queue.
2. In the Job Number field, type the job ID of the print job.
3. If the print job you want to delete is not yours, change the user ID in the User Name field to that of the owner of the print job.
4. Press ENTER.

The print job is deleted from the print queue.

Note: Security considerations on the remote host could prevent users from deleting any or all entries on a print queue. For example, on Windows NT, the Security tab of the printer's Properties controls authorizations for user access to the printer and its queue. On some UNIX systems, a user name of ROOT is required o delete entries of the printer queue.

Sending a Test Print

To send a test print to a target printer, do this:

1. At the TCP/IP : Line Printer (LPD) Diagnostics Menu, select option **PR** - Send a Test Print to a Printer.
2. Complete any required fields on the panel.
3. Press ENTER.

The test print is printed at the specified printer and a message is displayed to indicate this.

```
PROD---------------- TCP/IP : Line Printer (LPD) Diagnostics --------------/LPD
Select Option ===>
IPLP9103 PRINT REQUEST COMPLETED
   Q   - Query Print Queue
   D   - Delete a Job from the Print Queue
   PR  - Send a Test Print to a Printer
   X   - Exit

Host Name/Addr .. 199.0.90.189                          ( Required ALL )
Printer Name .... printer01                             ( Required ALL )
Job Number ......                                       ( Required D )
User Name ....... USER01                                ( Required D )
Link Name ......+                                       ( Optional ALL )
```

Chapter

17

Producing Reports

This chapter contains the following topics:

- About Reports
- Listing and Viewing Reports
- Searching the TCP/IP Events Database
- Searching Sampled Performance Data
- Extracting Data to a File
- Printing Reports
- Defining Printed Reports
- Long-range Reporting Using the Offline Archival System

About Reports

NetMaster for TCP/IP provides the following types of reports:

- Online reports (including a print facility)—that provide information about FTP, Telnet, connection, and Cisco channel card events from the events database
- Real-time performance reports—that provide real-time information about the sampled performance of IP nodes and the Cisco channel cards
- Near-time and past performance reports—that provide near-time and past information about the sampled performance and network events

Online Reporting

NetMaster for TCP/IP collects network data such as the volume of activity in a certain time period, or about the most active FTP users in the last day. This data can help you monitor network trends for preventive maintenance purposes to avoid performance problems.

The TCP/IP Reporting function is a data collection facility that extracts network activity data from the TCP/IP environment, writes these records to a database, and produces online reports. This function also allows you to extract the data for analysis by exporting it to other data analysis and reporting tools such as Microsoft Excel.

The Reporting Function produces online reports by performing a search with specified criteria. It allows you to do the following tasks:

- List and view predefined reports about FTP, Telnet, connection, and Cisco channel card events.
- Use predefined search criteria to produce event reports.
- Define your own searches to produce event reports.

To enable NetMaster for TCP/IP to collect the events, use the IPMONITOR parameter in ICS (see the *NetMaster for TCP/IP Administrator Guide* for details).

Note: Depending on your site-specific implementation, the same information about Telnet, FTP, and connection activities is also available in the Activity Log and transient logs.

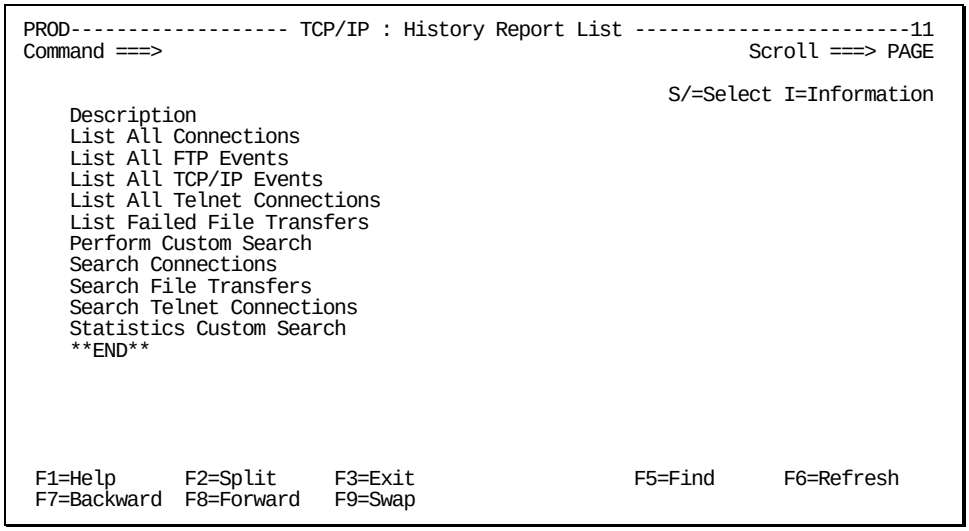
Listing and Viewing Reports

The following predefined reports are available:

- All connections
- All FTP Events
- All TCP/IP Events
- All Telnet Connections
- Failed File Transfers

To access these reports, do this:

1. Enter **/IPHIST.B** at a ===> prompt. The History Report List is displayed.



2. Enter **S** next to the report you want. The selected report is displayed.

Actions on the History Report List

The actions on the predefined reports are described below.

S or / (Select)—Displays the selected report

I (Information)—Displays application details such as Appl ID, Type, Name, Description, and Comments, that describe how the report is defined to NetMaster for TCP/IP. For information about these fields, press F1 (Help).

Searching the TCP/IP Events Database

The search facility allows you to either use predefined search criteria, or define your own search criteria, to obtain specific information from the TCP/IP events database.

Searching Connections

To search for connection events:

1. Enter **/IPHIST.B** at a ===> prompt. The History Report List is displayed, showing a list of available predefined searches.
2. Enter **S** next to Search Connections.

   The Connection Search Criteria panel is displayed, allowing you to perform a predefined search on any of these fields:

   From/To Date—The range of dates (in *dd/mm/yy* format) when records were written to the events database

   From/To Time—The range of time (in *hh:mm* format) when records were written to the events database

   Application Name—The name of the application being used by the connections you are searching for

   Job Name—The job or task name that is the OS/390 end of the connections. The values in this column match the Task Name (or mask) entered on the Diagnose Connections Menu.

   Bytes In Over/Under—The lower and upper bounds for the number of bytes received from the foreign host on the connections

   Bytes Out Over/Under—The lower and upper bounds for the number of bytes sent to the foreign host on the connections

   Remote IP Address—The remote address of the connections

   Remote Port—The remote port number being used by the connections

   Local IP Address—The local IP address being used by the connections

   Local Port—The local port number being used by the connections
3. Press F6 (Action) to activate the search.

Searching File Transfer Events

To search for file transfer (FTP) events using predefined criteria:

1. Enter **/IPHIST.B** at the ===> prompt. The History Report List is displayed, showing a list of available predefined searches.
2. Enter **S** next to Search File Transfers.

   The File Transfer Search Criteria panel is displayed, allowing you to perform a predefined search on any of these fields:

   Byte count over/under *n* bytes—Number of bytes transferred in an FTP request that are over or under the specified number of bytes.

   Dataset Name—Name of the FTP dataset.

   Duration Over *n* Seconds—All transmissions of a duration over the specified seconds.

   From/To Date—The range of dates when records were written to the events database.

   From/To Time—The range of time when records were written to the events database.

   Remote IP Address—For a server, the IP address of the client; for a client, the IP address of the server.

   User ID—On the client side, the ID of the local user who initiated the file transfer; on the server side, the ID of the remote user.
3. Press F6 (Action) to activate the search.

Searching Telnet Connections

To search for Telnet connection events using predefined criteria:

1. Enter **/IPHIST.B** at a ===> prompt. The History Report List is displayed, showing a list of available predefined searches.
2. Enter **S** next to Search Telnet Connections.

   The Telnet Connection Search Criteria panel is displayed, allowing you to perform a predefined search on any of these fields:

   From/To Date—The range of dates when records were written to the events database.

   From/To Time—The range of time when records were written to the events database.

   Duration Under *n* Seconds—All periods of less than the specified seconds between logon and logoff of any connections.

   LU Name—The name of the session in use on a particular LU.

Remote IP Address—The IP address of the remote host.

Connection Host Name—The name of the host (for example, CMCC7505 or ABCMVS1).

Connection Host Vendor—The host vendor name, for example, IBM (for IBM TCP/IP), CISCO (for a channel card), or TCPACCESS (for TCPaccess).

3. Press F6 (Action) to activate the search.

Performing a Custom Search

The Perform Custom Search option allows you to define your own search criteria for a custom search by using the fields from the events database.

Note: You can access the fields from the events database by entering **?** in the Field field on the Database Search Criteria panel.

To perform a custom search by defining your own search criteria, do this:

1. Enter **/IPHIST.B** at the ===> prompt. The History Report List is displayed, showing a list of available predefined searches.
2. Enter **S** next to Perform Custom Search. The Network Database : Search Criteria panel is displayed.
3. Complete the columns (see the examples below), and press F6 to perform the search. The TCP/IP : Event Log Search Results panel is displayed.

   Note: To display a selection list of values for an input column, enter **?** in the first blank field in the column.

Examples of Custom Searches

Use the following examples to help you customize your own searches of the events database.

Example 1

This is an example of search criteria that produced a list of all Telnet terminal sessions that lasted for less than 10 minutes from an IP address with the 202 prefix.

```
PROD---------------------- Network Database : Search Criteria ------------------
Command ===>                                                  Function=Search

                                                      D=Delete I=Insert R=Repeat
    "("   Field          Opr  Value                          Gen ")"   Bool
        + $IPRECTYPE   + =    TS                         +         + AND
        + $IPDURATION  + <    600                        +         + AND
        + $IPRMTADDR   + =    202                        + YES     +
        +              +                                 +         +
        +              +                                 +         +
```

Example 2

This is an example of search criteria that produced a list of all FTP events that failed.

```
PROD---------------------- Network Database : Search Criteria ------------------
Command ===>                                                  Function=Search

                                                      D=Delete I=Insert R=Repeat
    "("   Field          Opr  Value                          Gen ")"   Bool
    (   + $IPRECTYPE   + =    FS                         +         + OR
        + $IPRECTYPE   + =    FC                         +     )   + AND
        + $IPLASTREPL  + ¬=   2                          + YES     +
        +              +                                 +         +
        +              +                                 +         +
```

Example 3

This is an example of search criteria that produced a list of all file transfers for datasets with the SYS2 prefix.

```
PROD---------------------- Network Database : Search Criteria ------------------
Command ===>                                                  Function=Search

                                                      D=Delete I=Insert R=Repeat
    "("   Field          Opr  Value                          Gen ")"   Bool
    (   + $IPRECTYPE   + =    FS                         +         + OR
        + $IPRECTYPE   + =    FC                         +     )   + AND
        + $IPCOMMAND   + =    RETR                       +         + AND
        + $IPDSNAME1   + =    SYS2                       + YES     +
        +              +                                 +         +
        +              +                                 +         +
```

Example 4

This is an example of search criteria that, performed at the time of 4:00 pm produced a list of file transfers for the last hour.

```
PROD---------------------- Network Database : Search Criteria ------------------
Command ===>                                                  Function=Search

                                                      D=Delete I=Insert R=Repeat
    "("   Field          Opr  Value                              Gen ")"   Bool
    (   + $IPRECTYPE   + =    FS                                +         + OR
        + $IPRECTYPE   + =    FC                                +     )   + AND
        + $IPDATE      + =    24-NOV-1997                       +         + AND
        + $IPTIME      + >=   150000                            +         +
        +              +                                       +         +
        +              +                                       +         +
```

Actions on the Search Criteria Panel

The following editing actions are available:

D (Delete)—Deletes the current line.

I (Insert)—Inserts a blank line after the current line.

R (Repeat)—Copies and inserts a line after the current line.

Searching Sampled Performance Data

The primary purpose of the Statistics Custom Search is to help support staff to debug problems of other performance reports.

The Statistics Custom Search option allows you to perform a custom search on detailed performance data collected by the following Performance features:

- IP Node Monitor sampling
- TCP/IP Workload sampling
- Local Network Interface Workload sampling

The Statistics Custom Search allows you to find samples for particular resources to help diagnose unexpected results returned by the Performance features.

To access the Statistics Custom Search facility, do this:

1. Enter **/IPHIST.B** at a ===> prompt. The History Report List is displayed, showing a list of available predefined searches.
2. Enter **S** next to Statistics Custom Search.

   The Network Database : Search Criteria panel is displayed, allowing you to define your own search criteria. For information about how to use this panel, see the section “Performing a Custom Search”.

Extracting Data to a File

The events database that contains network activity data is retained in NetMaster for TCP/IP in the IPLOG dataset. This log is periodically archived to a comma-delimited file (IPDETAIL) for processing by external analysis and reporting tools. The period of time that data is kept online is defined by your System Administrator. For more information, see the *NetMaster for TCP/IP Administrator Guid*e.

You can analyze network activity and trends by reading the data extracted from the log and using any standard analysis and reporting tool on a PC.

To extract the network data on for purposes of analysis at other times, complete the following steps.

Note: You can also extract network data, by using the following command:

SUB BSYS $IPCALL ACTION=EXTRACT CLASS=IPLOG DATASET=*your.dataset.name*

1. Define a sequential dataset for the purpose of extracting the network data into this dataset. To do this:
   a. Access the ISPF/PDF Primary Menu.
   b. At the Option ===> prompt, enter **3.2.**
   c. At the Data Set Utility panel, select the **A** - Allocate New Data Set option, and complete the ISPF Library fields with your dataset specification.
   d. At the Allocate New Data Set panel, complete the allocation fields as shown below.

```
  Menu  RefList  Utilities  Help
--------------------------- Allocate New Data Set -----------------------------
  Command ===>


  Data Set Name . . . : NMIP.PROD.EXTRACT

  Volume serial . . . .                 (Blank for authorized default volume) *
  Generic unit. . . . . genuser         (Generic group name or unit address) *
  Space units . . . . . CYLINDER        (BLKS, TRKS, CYLS, KB, MB or BYTES)
  Primary quantity. . . 10              (In above units)
  Secondary quantity. . 10              (In above units)
  Directory blocks. . . 0               (Zero for sequential data set)
  Record format . . . . VB
  Record length . . . . 502
  Block size  . . . . . 0
  Expiration date . . .                 (YY/MM/DD, YYYY/MM/DD
                                         YY.DDD, YYYY.DDD in Julian form
   Enter "/" to select option            DDDD for retention period in days
     Allocate Multiple Volumes           or blank)

  ( * Only one of these fields may be specified)
```

2. Access the TCP/IP : History Data (enter **/IPHIST** at the ===> prompt).

3. At the ===> prompt, enter **EX** - Extract All TCP/IP Events to Dataset and, in the Extract DSN field, enter the dataset name you have just defined.

   The NetMaster system extracts all records from IPLOG in the events database (NDB) to the defined dataset, and presents them as comma-delimited fields with a header.

4. Transfer the defined dataset to your PC, and save it with a .CSV extension.
5. Use this .CSV file as input to your preferred PC application (for example, Microsoft Excel), and import this file as a comma-delimited format file.
6. Analyze your data by applying facilities such as graphs and charts, tables, and macros.

Printing Reports

The **P** (Printed Reports) option allows you to print reports currently defined to the NetMaster region. You can also use this option to define your own reports to print.

To display a list of predefined reports and print a selected report, do this:

1. Enter **/IPHIST.P** at a ===> prompt. The Report Writer : Report List is displayed.

```
PROD-------------------- Report Writer : Report List ------------------------10
Command ===>                                                    Scroll ===>

                                                        S/=Select I=Information
    Description
    All Connection Events - Detailed
    All Connection Events - Summary
    All FTP Events - Detailed
    All FTP Events - Summary
    All Telnet Events - Detailed
    All Telnet Events - Summary
    Connection Search - Detailed
    Connection Search - Summary
    Failed File Transfers - Detailed
    Failed File Transfers - Summary
    File Transfer Search - Detailed
    File Transfer Search - Summary
    Telnet Search - Detailed
    Telnet Search - Summary
    **END**
 F1=Help      F2=Split     F3=Exit                  F5=Find      F6=Refresh
 F7=Backward  F8=Forward   F9=Swap
```

2. Enter **S** next to the listed report you want to print. The Confirm Printer panel is displayed.
3. Press F6 to confirm the details of the print job.

If you selected any of the reports for *all* connection, FTP, or Telnet events, you are returned to the Report Writer : Report List panel, where a message is displayed indicating that the print job has been submitted to the print queue.

If you selected any of the other reports, the Connection Search Criteria panel is displayed and you can enter your search criteria to improve the search performance. For further information about using the Connection Search Criteria panel, see the section “Searching Connections”.

Checking the Print Queue

To check the print queue, at the ===> prompt on the Report Writer : Report List panel, enter **PQ**. The PSM : Output Queue is displayed.

Actions are available on this panel to allow you to browse a report output, release a held report, or delete a print job from the printer queue.

For more information about using Report Writer functions, see the *Management Services Report Writer User’s Guide.*

Defining Printed Reports

To set up you own reports to print, you must define them to the NetMaster for TCP/IP system. To define these reports, do this:

1. List all printed reports defined to NetMaster for TCP/IP by doing this:
   a. At the ===> prompt, enter **/MS.R.R.** The Report Writer : Report Definition Menu is displayed.
   b. At the ===> prompt, enter **L**; and in the Report Appl field, enter **$IP**. The Report Writer : Report Definition List for the specified application is displayed.
2. Copy a listed report that has a format similar to the report you want to set up. To do this, enter **C** next to the listed report you want to copy. The Report Writer : Report Description panel is displayed.
3. In the Report Name field, enter your own report name.
4. In the Description field, enter your report description.
5. So that the report you are setting up will be listed in the same report group as other NetMaster for TCP/IP printed reports, ensure that the Report Exit field has the **$IPLORWX** value, and the Group field has **$IPREPORTING** entered.

6. In the Criteria Name field, specify your own search criteria by accessing the CAS : Criteria Definition Menu. To do this, enter **/CAS.C** at the ===> prompt. The CAS : Criteria Definition Menu is displayed.

   Note: For details about using the CAS : Criteria Definition Menu, press F1 (Help). To file your definitions, press F3.

7. Change the title of your report by doing this:

   a. At the Report Writer : Report Definition List, type **LC** next to your report. The Report Writer : Report Definition Component List is displayed.

   b. Select the **RH** - Report Header option, then enter your own report title.

   c. To file the changes, press F3. The Report Writer : Report Definition Component Menu is displayed.

   d. Press F3 until you reach the Report Writer : Report Definition Menu.

   e. Select **R** - Reset Report Cache to immediately activate the new report definition.

Long-range Reporting Using the Offline Archival System

The records written to the IPLOG Events database can optionally also be written to your SMF files.

Records written to the SMF files are stored in an offline archival system that can be extended by IBM and third-party products such as SLR and SAS.

This system archives detail data (both current active SMF records and offline SMF archives) over periods of several months and serves as an aid to long-term network and capacity planning.

For details of the SMF record format produced by NetMaster for TCP/IP, see the *NetMaster for TCP/IP Administrator Guide*.

To access these records, you can customize and use your preferred SMF reporting facilities such as the following:

- Batch jobs created and run in TSO
- REXX procedures
- CLISTS
- SLR
- SAS

Information for these processes is outside the scope of this guide.

Chapter

18

Reporting Real-time Performance

This chapter contains the following topics:

- Monitoring Real-time Performance
- Displaying Performance History
- Listing Resource Attributes of Performance Samples
- Diagnosing Resource Attributes

Monitoring Real-time Performance

NetMaster for TCP/IP provides facilities to monitor performance and capacity in OS/390 and z/OS TCP/IP networks.

You can access a collection of performance facilities from the IP resource monitor and the IP node monitor.

These facilities include real-time reports of performance samples for IP nodes, Cisco channel cards, and other host and network resources. These reports provide a graphical representation of recent performance history of the attributes of a network resource being monitored. The available graphs provide the following information:

- Details of the last 12 samples
- Summary of samples from the last 24-hour period

Displaying Performance History

To access real-time reports, enter **H** (Show Performance History) next to an IP node or IP resource on the following displays:

- IP resource monitor (/IPMON)
- IP node monitor (/IPNODE)
- Trace route list (option TR from /IPDIAG)
- Device links

For details of the information displayed and the actions available on performance monitor panels, press F1 (Help).

Note: In some displays, attributes are grouped by qualifier; in other displays, qualifiers are grouped by attribute. If the column heading is Attribute/Qualifier, the records are grouped by attribute, and each attribute can be expanded to show its component qualifier records. If the column heading is Qualifier/Attribute, the records are grouped by qualifier and each qualifier can be expanded to show its component attribute records.

Some displays are expanded when initially presented to show all items (attributes or qualifiers) within each group. Some displays are collapsed, so that only ungrouped items and groups containing a single item are expanded. The expanded group line displays totals for all items in the group.

```
PROD--------------- TCP/IP : Monitor Address Space Performance ----------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... TCPIP01
     Description ......... TCP/IP Application
     Current Alerts ...... 0
                                        E=Expand C=Contract  S/=Summary D=Detail
                               --- Alerts ---           Last
    Qualifier/Attribute        Current  Total  Samples  Sample            Value
     |-- TCPIP01                           0      114  16:44                -
       |-- CPU%                            0       19  16:44               10
       |-- EXCP                            0       19  16:44             2046
       |-- JOBCOUNT                        0       19  16:44                1
       |-- SRBCPU                          0       19  16:44              349
       |-- TASKCPU                         0       19  16:44            54856
-------------------------------------------------------------------------------
                                        E=Expand C=Contract  S/=Summary D=Detail

    Qualifier/Attribute         Type       Description
     |-- TCPIP01                GAUGE
       |-- CPU%                 GAUGE      CPU percentage
       |-- EXCP                 GAUGE      Change in EXCP count
       |-- JOBCOUNT             GAUGE      Number of jobs aggregated in this sa
       |-- SRBCPU               GAUGE      Change in SRB CPU Used (ms)
       |-- TASKCPU              GAUGE      Change in Task CPU Used (ms)
-------------------------------------------------------------------------------
                                        E=Expand C=Contract  S/=Summary D=Detail

    Qualifier/Attribute         Message
     |-- TCPIP01
       |-- CPU%
       |-- EXCP
       |-- JOBCOUNT
       |-- SRBCPU
       |-- TASKCPU
```

Listing Resource Attributes of Performance Samples

The performance history panels display the attributes that are being monitored for a network resource (such as an IP node, an OSA card, or a Cisco channel card) and provide details for each listed resource. The resource details for each listed attribute include:

Total number of alerts generated when the values of monitored attributes fall beyond the threshold defined by your network administrator

- Number of times the same alert was generated since the region was started
- Total number of samples taken
- Date and time of last sample
- Value presented by the processing of raw sampled data
- Type of processing of the raw sampled data to produce the value presented (see the section “Diagnosing Resource Attributes”)
- Description of the attribute
- Messages

Diagnosing Resource Attributes

The Resource Summary Graph and Resource Detail Graph panels allow you to view information about performance samples collected over a time period.

There are two types of display:

- Numeric values (for example, network response time or number of bytes transferred on a connection)
- List of values (for example, network status)

Information on the Bar Charts

The bar charts present information resulting from the following types of processing of raw sampled data:

- Gauge (for example, the round-trip time of a ping in milliseconds)—a gauge value is displayed as an absolute value.
- Rate (for example, the number of errors per hour)—a counter value is displayed as a rate of change of a counter per period.
- Enumerated Value (for example, a status value)—a discrete value is displayed as an occurrence of that particular value. Each occurrence of the value may be aggregated so that a percentage of that value over time is available.
- Total (displayed for the workload performance options)—a count that is totaled and then reset every hour to zero.

Information on the bar charts is presented in ascending order of time. The bar charts are updated automatically as new sample data is collected.

When a sampled value is within a predefined threshold set for that resource, the value is displayed in green. Any detail sample that causes an alert is displayed in one of the following colors:

- Red if the value is beyond the set alert threshold.
- Yellow if the value is between the high-alert value and the reset value for the high alert, or between the low-alert value and the reset value for the low alert.

A value of N / A indicates that the sample could not be taken.

Displaying the Resource Summary Graph

The Resource Summary Graph consists of sampled values collected over 24 hours at hourly intervals.

To access this graph from a performance monitor panel, enter **S** beside the selected attribute. The Resource Summary Graph is displayed.

For details of the information displayed and the actions available, press F1 (Help).

```
PROD------------ NetMaster : Resource Summary Graph (Gauge) ------------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... TCPIP01
     Description ......... TCP/IP Application
     Attribute ID......... CPU%(CSNM2)
     Description ......... CPU percentage
     Total Alert Count ... 0
     Period .............. 3hrs 0mins : 08-AUG-2001 from 10:00 to 13:00

                       Axis range is 1 to 10, each 5 points is 1
    Start Time   Value ----1----2----3----4----5----6----7----8----9----10
    10:00            0
    11:00            4 ■■■■■■■■■■■■■
    12:00            3 ■■■■■■■■■■
    13:00            2 ■■■■■■■
    **END**
```

Displaying the Resource Detail Graph

The Resource Detail Graph consists of values from the last 12 samples taken at short fixed intervals (set at between 5 and 60 minutes).

To access this graph from a performance monitor panel, enter **D** beside the selected attribute. The Resource Detail Graph is displayed.

For details of the information displayed and the actions available, press F1 (Help).

```
PROD-------------- NetMaster : Resource Detail Graph (Gauge) ------------------
Command ===>                                                  Scroll ===> PAGE

     Resource ID ......... TCPIP01
     Description ......... TCP/IP Application
     Attribute ID......... CPU%(CSNM2)
     Description ......... CPU percentage
     Total Alert Count ... 0
     Period .............. 3hrs 59mins : 08-AUG-2001 from 10:40 to 14:39

                       Axis range is 1 to 10, each 5 points is 1
    Sample Time  Value ----1----2----3----4----5----6----7----8----9----10
    10:40            0
    11:39            5 ■■■■■■■■■■■■■■■■■
    12:39            3 ■■■■■■■■■■■
    13:39            3 ■■■■■■■■■
    14:39            3 ■■■■■■■■■
    **END**
```

Chapter

19

Diagnosing IP Networks

This chapter contains the following topics:

- Network Diagnosis Functions Menu
- Browsing System Information
- Browsing the Interface List
- Displaying a Routing Table
- Viewing SNMP Functions

Network Diagnosis Functions Menu

To display the Network Diagnosis Functions menu, enter **/IPDIAG** at a ===> prompt.

The Network Diagnosis Functions menu comprises several options that enable you to monitor the activity of IP hosts in the IP network.

```
PROD---------------- TCP/IP : Network Diagnosis Functions -------------/IPDIAG
Select Option ===>

   P    - Ping                                              PING
   TR   - Trace Route                                       -
   PT   - Packet Tracing                                    IPPKT
   S    - Show Host System Information                      -
   I    - Show Local Interfaces                             -
   R    - Show Routing Table                                -
   TN   - Start a Telnet Connection                         -
   SF   - Perform SNMP Functions                            -
   X    - Exit

Host Name/Addr   ________________________________________  ( Req P TR S I R TN )
Net Address Mask ________________                         ( Opt R )
Community Name   ________________________________________  ( Opt S I R )
Link Name .....+ ____________                             ( Opt All )
```

Network Diagnosis Functions Menu Options

For information about the tasks that you can perform from the Network Diagnosis Functions menu, press F1 (Help).

Input Fields on the Network Diagnosis Functions Menu

The fields on the Network Diagnosis Functions menu are:

Host Name/Addr—The exact name or address of the host (that is, the address of the IP node) that you want to diagnose. (Required for the P, TR, S, I, R, and TN options)

Net Address Mask—You can enter a single network address or use a mask to determine what is to be displayed on the Routing Table. By using masking, you will experience a considerable performance improvement when displaying the Routing Table. (Optional for R)

Community Name—You can specify the SNMP community name. This is a type of password that determines whether you can use the System Information, Interfaces, Routing Table, and MIB-II actions which all use SNMP (the community name is sent to the host along with your request for information).

The default community name is *public* (in lower case). The name is case sensitive.

Community names can be registered by the NetMaster for TCP/IP systems administrator so that they do not have to be re-entered at each use. (For information about registering community names, see the *Unicenter NetMaster Network Management for TCP/IP Administrator Guide*.) (Optional for S, I, and R options)

Note: If the host does not accept the community name, no information is provided and your request will timeout after about 15 seconds.

Link Name—You can perform IP network diagnosis on a remote NetMaster for TCP/IP system by specifying the name of the INMC link to that system. If you are unsure of a link name, enter a question mark (**?**) in this field to display a list of the names of all linked systems running NetMaster for TCP/IP—this list contains the host names of the linked systems. (Optional for All)

Browsing System Information

To browse system information for a selected IP host (for example, a router):

1. Select option **S** - System Information from the Network Diagnosis Functions menu (/IPDIAG).

   Note: You can also access system information from the IP node monitor. To do this, type **S** next to the entry on the IP node monitor.

2. Enter a Community Name (optional).

3. Press ENTER. The System Information panel is displayed.

Note: The system information facility uses SNMP MIB-II technology, which is not supported by all hosts. SNMP must be supported on a router for you to be able to view system information about it.

```
PROD-------------------- TCP/IP : System Information ----------Columns 001 079
Command ===>                                                  Scroll ===> PAGE

******************************** TOP OF DATA ********************************
IP Address ............. 123.168.1.1
Host Name .............. Hubble
Name ................... HUBBLE 4500

Type ................... cisco4500
Description ............ Cisco Internetwork Operating System Software
                         IOS (tm) 4500 Software (C4500-DR-M), Version 11.1(5),
                         Copyright (c) 1986-1996 by cisco Systems, Inc.
                         Compiled Mon 05-Aug-96 14:16 by mkamson
Contact ................
Location ...............

Up time ................ 143 Days 03:10:09.62
Services ............... Router, Datalink

CPU Utilization % ...... 2
CPU 1 Minute Average ... 3
CPU 5 Minute Average ... 3
```

For details of the information displayed, press F1 (Help).

Browsing the Interface List

To view a list of interfaces for a selected IP host:

1. Select option **I** - Interface List from the Network Diagnosis Functions menu (/IPDIAG).
2. Enter a host name or address in the Host Name/Addr field.
3. Enter a Community Name (optional).
4. Press ENTER. The Interface List panel is displayed.

Note: The interface list facility uses SNMP MIB-II technology, which is not supported by all hosts.

```
PROD---------------------- TCP/IP : Interface List ----------------------------
Command ===>                                                  Scroll ===> CSR

Interfaces on Host ... Hubble
           Address  199.0.80.25
    IF                      -------------- Status -------------- Time In State
    No Description          Admn Oper Prot Reason                Days hh:mm:ss
     1 IBM LCS              up   up                                 3 16:11:12
     2 IBM LCS              down down                               3 16:11:12
     3 Channel to channel   up   up                                 3 16:11:12
     4 Channel to channel   up   up                                 3 16:11:12
     5 IBM IP-over-PVM link down down                               3 16:11:12
     6 IBM IP-over-PVM link down down                               3 16:11:12
    **END**
-------------------------------------------------------------------------------
    IF                           ----- Inbound ------ ------- Outbound --------
    No Description        Reliab    Bytes Drops Error    Bytes Drops Error Qlen
     1 IBM LCS                    294542K     0     0  396540K     0   137    0
     2 IBM LCS                          0     0     0        0     0     0    0
     3 Channel to channel             961K     0     0    5498K     0     0    0
     4 Channel to channel            5758K     0     0    6674K     0     0    0
     5 IBM IP-over-PVM link             0     0     0        0     0     0    0
     6 IBM IP-over-PVM link             0     0     0        0     0     0    0
    **END**
-------------------------------------------------------------------------------
    IF                      --------- Link Details ----------
    No Description          MTU    Speed    Physical Address  Type
     1 IBM LCS              2048   4M       374040D540        tokenRing
     2 IBM LCS              1500   10M                        Ethernet
     3 Channel to channel   8520   4500K                      -
     4 Channel to channel   8520   4500K                      -
     5 IBM IP-over-PVM link 8520   56K                        -
     6 IBM IP-over-PVM link 8520   56K                        -
    **END**
```

The Interface List panel displays details of each interface for the selected host. For details of the information displayed, press F1 (Help).

Displaying a Routing Table

A routing table holds a list of paths through which hosts can communicate with each other. To view the routing table for a device, select option **R** - Routing Table from the Network Diagnosis Menu (optionally placing a mask in the Net Address Mask field, and optionally typing a Community Name), and press ENTER. The Routing Table panel is displayed.

Note: The routing table facility uses SNMP MIB-II technology, which is not supported by all hosts.

```
PROD------------------------ TCP/IP : Routing Table -------------------------
Command ===>                                                 Scroll ===> PAGE

Routing Table on Host ... Hubble
                  Address  192.168.1.1
Net Address Mask ........                        Matching Entry 1 of 25
 P=Ping TN=Telnet S=Sys Info NL=Name Lookup I=Interfaces R=Routing Tab M=MIB-II
    Net Address     First Hop       Link        Subnet Mask     Subnet Value
    Default         123.168.80.5    Serial1
    123.168.80.4    123.168.80.5    Serial1     255.255.255.252
    123.168.80.24   <direct>        TokenRing0  255.255.255.252
    123.168.80.32   123.168.80.5    Serial1     255.255.255.252
    123.168.81.0    <direct>        Ethernet0   255.255.255.0
    123.168.82.0    123.168.80.5    Serial1     255.255.255.0
    123.168.83.0    123.168.80.5    Serial1     255.255.255.0
    123.168.84.0    123.168.80.5    Serial1     255.255.255.0
    123.168.85.0    123.168.80.5    Serial1     255.255.255.0
    123.168.86.0    123.168.80.5    Serial1     255.255.255.0
-------------------------------------------------------------------------------
    Net Address     First Hop       Link                    Routing Protocol
    Default         123.168.80.5    Serial1                 rip
    123.168.80.4    123.168.80.5    Serial1                 rip
    123.168.80.24   <direct>        TokenRing0              local
    123.168.80.32   123.168.80.5    Serial1                 rip
    123.168.81.0    <direct>        Ethernet0               local
    123.168.82.0    123.168.80.5    Serial1                 rip
    123.168.83.0    123.168.80.5    Serial1                 rip
    123.168.84.0    123.168.80.5    Serial1                 rip
    123.168.85.0    123.168.80.5    Serial1                 rip
    123.168.86.0    123.168.80.5    Serial1                 rip
```

You might find that the number of entries in your Routing Table is such that it becomes unmanageable. If this is the case, you can reduce the list by entering a network address or network address mask and using the REFRESH command (F6) to rebuild the list.

For details of the information displayed, press F1 (Help).

Actions on the Routing Table

The following actions can be applied to routers appearing in the First Hop column of the routing table:

I (Interfaces)—presents the Interface List panel for a selected router. To apply the Interfaces action, enter **I** to the left of the appropriate routing table entry on the list. For more information about the interface list, see the section “Browsing the Interface List”.

M (MIB-II)—presents the TCP / IP : MIB-II Access Menu. To apply the MIB-II action, enter **M** to the left of the appropriate routing table entry on the list. The IP address of the first hop is placed in the IP Address field on the MIB-II Access Menu.

NL (Lookup)—returns the full name of the selected router.

P (Ping)—executes the PING command that tests whether the first hop address is reachable. To apply the Ping action, enter **P** to the left of the appropriate routing table entry on the list.

R(Routing Table)—presents the routing table for the router listed in the First Hop column. You can use the Net Address Mask field to limit the presented list. For more information, see the section “Displaying a Routing Table”.

S (System Information)—presents the TCP / IP : System Information panel for a selected first hop address. To apply the System Information action, enter **S** to the left of the appropriate routing table entry on the list. For more information about system information, see the section “Browsing System Information”.

TN (Telnet)—initiates a Telnet connection to the router listed in the First Hop column. You can use this connection to enter commands on that router to determine and alter its state.

Viewing SNMP Functions

If you need to access further management information about IP hosts by means of SNMP, you can access the SNMP : Function Menu direct from the Network Diagnosis Functions menu.

To access the SNMP functions, select the **SF** - SNMP Functions option from the Network Diagnosis Functions menu and press ENTER. The SNMP : Function Menu is displayed.

```
PROD----------------------- SNMP : Function Menu ----------------------$SP003
Select Option ===>

   M   - Access MIB-II                                        SNMP
   P   - Ping a Device                                        -
   T   - Trace a Network Route                                -
   R   - List Managed Resources (OpenView and NetView only)   -
   A   - Manager Administration List                          -
   X   - Exit

SNMP Manager Name .........+ ________           ( Required R Optional M P T )
             Description ...

Device Name ................ ________________________________________________
                             ________________________________________________
       IP Address .......... ________________
```

For further information about using the SNMP : Function Menu, press F1 (Help).

Chapter

20

Collecting and Using Trace Data

This chapter contains the following topics:

- Tracing IP Packets in TCP/IP
- Packet Tracing Menu
- Performing a Trace and Saving Data
- Starting CTRACE
- Starting a Trace
- Stopping a Trace
- Stopping CTRACE
- Saving the CTRACE Data
- Viewing the Saved Packet Trace
- Listing Saved Traces
- Updating Packet Trace Description
- Listing IP Addresses Within a Trace
- Listing Connections Within a Trace
- Listing Packets in a Selected Trace
- Viewing Data for a Selected Packet
- Errors in Packets

Tracing IP Packets in TCP/IP

The packet tracing facility of NetMaster for TCP/IP includes the following features:

- Ability to start and stop CTRACE (Component Trace)

  CTRACE is a service aid that is distributed by IBM. It allows you to record and diagnose system and program problems. For further information, see the *OS/390 MVS Diagnosis: Tools and Service Aids* manual.

- Ability to trace IP packets with specified criteria
- A trace format and display facility
- Ability to display active traces
- An archive of trace information

The packet tracing facility can be used with both IBM and TCPaccess stacks.

Packet Tracing Menu

To display the Packet Tracing Menu, enter **/IPPKT** at a ===> prompt.

The Packet Tracing Menu comprises several options that enable you to trace packets, and to save and view details of your traces.

```
PROD-------------------- TCP/IP : Packet Tracing Menu ------------------ /IPPKT
Select Option ===>

   S   - Start CTRACE
   PT  - Packet Trace
   LA  - List Active Traces
   PTC - Packet Trace Clear
   P   - Stop CTRACE
   SV  - Save Trace Data
   L   - List Saved Traces
   X   - Exit

Host Name/Addr ...                                        ( Optional PT )
Link Name .......+                                        ( Optional All )
```

Packet Tracing Menu Options

The tasks that you can perform from this menu are shown in the following table, which also indicates where you can find a detailed description of these tasks in this chapter:

To perform the task ...	Use option ...	Described in the section...
Preparing for tracing by starting the Component Trace CTRACE	**S**	"Starting CTRACE"
Starting a packet trace	**PT**	"Starting a Trace"
Listing active traces	**LA**	"Listing Active Traces"
Stopping a packet trace	**PTC**	"Sequence of Actions"
Stopping the CTRACE	**P**	"Stopping CTRACE"
Saving trace data ready for use	**SV**	"Saving the CTRACE Data"
Listing saved traces and viewing details of individual packets in a selected trace	**L**	"Listing Saved Traces" and "Viewing the Saved Packet Trace"

Input Fields on the Packet Tracing Menu

Host Name/Addr—You can restrict the scope of the trace by entering the name or address of the host for which you want to trace packets. If you do not specify a value, then all connections are traced.

(Optional for menu option PT)

Link Name—You can invoke packet trace functions on a remote NetMaster for TCP/IP system by specifying the name of the INMC link to that system. If you are unsure of a link name, type a question mark (**?**) in this field and press ENTER to display a list of the names of all linked systems running NetMaster for TCP/IP—this list contains the host names of all of the linked systems.

(Optional for all menu options)

Performing a Trace and Saving Data

To perform a trace and save the trace data:

1. Start CTRACE.
2. Start a trace.
3. Reproduce the problem you are tracing.
4. Stop all traces.
5. Stop CTRACE.
6. Save the packet trace data.

You can also see what traces are currently running, and view trace data that has been saved.

These actions are described in the following sections.

Sequence of Actions

The options on the Packet Tracing Menu are listed in the order in which you would normally use them.

If you already have a CTRACE dataset that contains a TCP/IP packet trace, you can view the trace by firstly saving the trace data by using option SV and then using option L to list the saved traces.

For ease of reference, the information in this chapter is presented in the same order as the options on the Packet Tracing Menu.

Starting CTRACE

Before you can begin tracing packets, you need to start CTRACE (Component Trace).

To start CTRACE, do the following:

1. Enter **S** (Start CTRACE) at the ===> prompt on the Packet Tracing Menu. The Start CTRACE panel is displayed.

Start CTRACE Panel (IBM TCP/IP)

```
PROD------------------------- TCP/IP : Start CTRACE ------------------------
Command ===>

CTRACE will be started with the following command.

Press F6 to Action or F12 to Cancel

Command to Start CTRACE ... TRACE CT,WTRSTART=PTTCP,NOWRAP
```

Start CTRACE Panel (TCPaccess)

```
PROD----------------------- TCP/IP : Start CTRACE ----------------------------
Command ===>

CTRACE will be started with the following trace job and command.

Press F6 to Action or F12 to Cancel

TCPaccess Trace Job.................. TCPTRC52

Command to Start TCPaccess CTRACE ... TRACE CT,WTRSTART=PTTCP,NOWRAP
```

2. Modify the contents of the Command to Start CTRACE field, if necessary. This is the command that NetMaster for TCP/IP issues to the operating system to start CTRACE.

   Note: To trace TCP/IP packets, CTRACE must be configured with the relevant trace options. For information, see the "Advanced Configuration Tasks" chapter in the *NetMaster for TCP/IP Administrator Guide.*

3. Press the Action key (F6) to start CTRACE.

   The CTRACE START command and TCPaccess trace job values are saved when you press the Action key. These saved options are then used as defaults next time you use this panel.

   NetMaster for TCP/IP issues the command specified in the command field. It then automatically responds to the WTOR (Write to Operator with Reply) messages written to the console during CTRACE start processing.

Note: If any errors are encountered when starting CTRACE, error information may be written to the activity log. To view this log, enter **/LOG** at the ===> prompt.

Starting a Trace

Once you have started CTRACE, you can then begin tracing data.

You can start a trace from any of the following panels:

- Packet Tracing Menu
- Telnet Connection List
- Connection List

Starting a Trace from the Packet Tracing Menu

One of the places where you can start tracing packets is the Packet Tracing Menu.

To start a trace from this menu, do the following:

1. Select option **PT—**Packet Tracing.
2. To limit your trace to a specific host name or address, enter a value in the Host Name/Addr field.

   Note: If you do not enter a value in this field, then you start a trace of all connections. Tracing all connections may produce a large amount of output and may affect system performance.
3. To start a packet trace on a remote NetMaster for TCP/IP system, specify the name of the INMC link to that system in the Link Name field.
4. Press ENTER. A message is returned, advising you that the trace has started. An example of such a message is:

   ```
   IPGP3109 PACKET TRACE STARTED WITH
   'PKT,LINKNAME=*,ON,FULL,IP=123.123.123.123'
   ```

Note: If you want to trace more than one specific host, repeat these steps for each host name.

Starting a Trace from a Connection List

You can start a trace directly from either of the following connection lists, by applying the PT action to a listed connection:

- Telnet Connection List
- Connection List (for a task)

Listing Active Traces

To find out what traces you have started, you can list active traces whenever any are running.

To list active traces, do the following:

1. Select option **LA—**List Active Traces from the Packet Tracing Menu.
2. To list active packet traces on a remote NetMaster for TCP/IP system, enter the name of the INMC link to that system in the Link Name field.
3. Press ENTER. The Active Packet Trace List is displayed.

```
PROD-------------------- TCP/IP : Active Packet Trace List --------------------
Command ===>                                                  Scroll ===> CSR
                                                          PTC=Packet Trace Clear

    Foreign Host    Lport
    123.123.81.25   *
    123.123.77.55   *
    **END**
```

Stopping a Trace

Before you can save your trace data, you must first stop tracing packets, and then stop CTRACE.

You can stop a trace from any of the following panels:

- Packet Tracing Menu
- Telnet Connection List
- Connection List

Stopping a Trace from the Packet Tracing Menu

One of the places where you canstop a trace is the Packet Tracing Menu.

To stop a trace from this menu, do the following:

1. Select option **PTC**—Packet Tracing Clear.
2. To stop traces on a remote NetMaster for TCP/IP system, specify the name of the INMC link to that system in the Link Name field.
3. Press ENTER. The Confirm Stop panel is displayed.

```
PROD------------------------ TCP/IP : Confirm Stop --------------------------
Command ===>


             +-------------------------------------------------+
             | Press F6 to confirm Trace Stop for all Links    |
             | Press F12 to cancel                             |
             +-------------------------------------------------+
```

4. Press the Confirm key (F6). The Packet Tracing Menu is displayed, with a message confirming that a trace stop has been issued. This action stops all packet tracing. An example of such a message is:

   ```
   IPGP3110 PACKET TRACE STOPPED WITH 'PKT,LINKNAME=*,OFF'
   ```

Stopping a Trace from a Connection List

You can stop a trace directly from either of the following connection lists, by applying the PTC action to a listed connection:

- Telnet Connection List
- Connection List

Stopping CTRACE

When you have done all of the tracing you need, and have stopped tracing packets by issuing the PTC command, you then need to stop CTRACE before you can save the trace records.

To stop CTRACE, do the following:

1. Select option **P**—Stop CTRACE on the Packet Tracing Menu.
2. To stop CTRACE on a remote NetMaster for TCP/IP system, specify the name of the INMC link to that system in the Link Name field.
3. Press ENTER. The confirmation panel Stop CTRACE is displayed.

```
PROD-------------------------TCP/IP : Stop CTRACE -----------------------------
Command ===>

              +-------------------------------------------------+
              |        You are about to stop CTRACE.            |
              |                                                 |
              | Press F6 to confirm CTRACE Stop                 |
              | Press F12 to cancel                             |
              +-------------------------------------------------+
```

4. Press the Action key (F6) to confirm that you want to stop CTRACE. The Packet Tracing Menu is displayed, with a message confirming that CTRACE has stopped.

Note: Once you have stopped CTRACE, you need to start it again if you want to run another trace.

Saving the CTRACE Data

When you have stopped CTRACE, you can save the CTRACE records to the NetMaster for TCP/IP database. You need to do this so that you can view the traced packets.

To save your trace data, do the following:

1. Select option **SV** (Save Trace Data) on the Packet Tracing Menu.
2. If you want to stop traces on a remote NetMaster for TCP/IP system, enter the name of the INMC link to that system in the Link Name field.

   Note: The trace data is saved on the remote system if a link name is specified.
3. Press ENTER. The confirmation panel Save Trace Data is displayed.

```
PROD---------------------- TCP/IP : Save Trace Data --------------------------
Command ===>


The trace data will be obtained from the following trace dataset.

Press F6 to Action or F12 to Cancel


Trace Dataset Name ... SYS1.TRACE
```

4. Press the Action key (F6) to confirm that you want to save the trace data.

   When the save processing has completed you are returned to the Packet Tracing Menu, with a message indicating:

   - How many IP packets were in the trace data that you saved
   - How many trace records were read during the save processing

Note: If major errors (such as missing records or invalid packet headers) are found during the save processing, the Save Trace Warnings/Errors panel is displayed.

If the number of CTRACE records read is a lot more than you were expecting, it may be worth checking that you have CTRACE configured with the correct trace options. To trace TCP/IP packets, the following trace options are required:

```
TRACE=USRP
USR=(5E4)
```

```
PROD---------------- TCP/IP : Save Trace Warnings/Errors ------Columns 001 079
Command ===>                                  Function=BROWSE Scroll ===> CSR
IPPT6207 ERRORS/WARNINGS ISSUED DURING SAVE OF TRACE FILE
****************************** TOP OF DATA ******************************
IPPT6211 *WARNING* UNEXPECTED SEQUENCE NUMBER. EXPECTED: 2 GOT: 3
IPPT6208 Description: CTRACE Trace Record Containing Unexpected Sequence Number
IPPT6209      000000 FFD7ADA8 73527892 1E00E5E4 00F75300 * P y   k  VU 7  *
IPPT6209      000010 E3C3D7C9 D7F3F140 03404B4B 1D4C3C4E *TCPIP31   .. < +*
IPPT6209      000020 E8002902 C0F042F4 E5859989 86A84040 *Y   {0 4Verify  *
IPPT6209      000030 404B4B1D 4C3C4E7D 002902C0 F042F440 * .. < +'   {0 4 *
IPPT6209      000040 40114F40 2902C0F0 42F43C4F C6402902 *  |   {0 4 |F   *
IPPT6209      000050 C0E842F7 4F3C4FD1 40614040 40403C4F *{Y 7| |J /     |*
IPPT6209      000060 5D7E4F3C 50504011 50502902 C0F042F4 *)=| &&  &&  {0 4*
IPPT6209      000070 3C50D640 2902C0E8 42F74F29 02C0E842 * &O   {Y 7|  {Y *
IPPT6209      000080 F6C6E3C9 40404029 02C0E842 F7614040 *6FTI     {Y 7/  *
IPPT6209      000090 40403C50 6D7E4F3C D1604011 D1602902 *   &_=| J-  J-  *
IPPT6209      0000A0 C0F042F4 3CD1E640 2902C0E8 42F74F3C *{0 4 JW   {Y 7| *
IPPT6209      0000B0 D1F06040 4040403C D17D7E4F 3CD2F040 *J0-     J'=| K0 *
IPPT6209      0000C0 11D2F029 02C0F042 F43CD2F6 402902C0 * K0  {0 4 K6   {*
IPPT6209      0000D0 E842F74F 2902C0E8 42F6C6E3 C9404040 *Y 7|  {Y 6FTI   *
IPPT6209      0000E0 2902C0E8 42F74040 403CD34D 7E4F3CD4 *  {Y 7    L(=| M*
IPPT6209      0000F0 404011D4 402902C0 F042F43C D4C64029 *   M   {0 4 MF  *
```

5. Print the Save Trace Warnings/Errors panel, using the PRINT command, as you cannot view these errors again after you leave this panel.

Note: The trace data displayed on this panel is held in a dataset with default name SYS1.TRACE. Data in this dataset is from all traces that were running.

Viewing the Saved Packet Trace

Once you have saved the packet trace data, you can view it. There are five levels of detail that you can view:

- The list of saved traces (see the section “Listing Saved Traces”)
- IP addresses in a selected trace (see the section “Listing IP Addresses Within a Trace”)
- All connections within a trace (see the section “Listing Connections Within a Trace”)
- The list of packets in a selected trace (see the section “Listing Packets in a Selected Trace”)
- Data for a selected packet (see the section “Viewing Data for a Selected Packet”)

Listing Saved Traces

To list the traces saved by your packet trace, do the following:

1. Select option **L**—List Saved Traces from the Packet Tracing Menu.
2. To list saved traces on a remote NetMaster for TCP/IP system, specify the name of the INMC link to that system in the Link Name field.
3. Press ENTER. The Saved Trace List is displayed.

```
PROD---------------------- TCP/IP : Saved Trace List --------------------------
Command ===>                                                 Scroll ===> CSR

          U=Update D=Delete S/I=IP Address List C=Connection List P=Packet List
    -------- Save Details -------- Packet
    Date        Time      UserID    Count Short Description
    10-JUL-2001 09:14:25  USER01      560 A test
    08-JUL-2001 16:10:30  USER02       41 My test of icmp to cs 2.5
    06-JUL-2001 11:25:38  USER03      581 First test
    03-JUL-2001 10:31:47  USER03      283 Second test
    30-JUN-2001 14:04:11  USER01      560 Third test
    11-JUN-2001 12:10:58  USER04      560
------------------------------------------------------------------------------
PROD---------------------- TCP/IP : Saved Trace List -------------------------
Command ===>                                                 Scroll ===> CSR

          U=Update D=Delete S/I=IP Address List C=Connection List P=Packet List
    Start       Start End   IP Addr
    Date        Time  Time    Count IP Addresses
    16-JUN-2001 11:12 11:13     >31 123.0.77.55 123.0.91.203 123.123.11.22 ...
    08-JUL-2001 16:09 16:10       2 123.0.77.55 123.123.11.22
    06-JUL-2001 11:24 11:24     >19 123.0.77.55 123.0.91.108 123.0.91.143 ...
    03-JUL-2001 10:28 10:30      25 123.0.0.10 123.0.77.30 123.0.77.55 ...
    16-JUN-2001 11:12 11:13     >31 123.0.77.55 123.0.91.203 123.123.11.22 ...
    11-JUN-2001 12:00 12:01       0
```

The Saved Trace List displays a list of traces that have been captured and loaded from CTRACE. The list is sorted (in reverse save-date and time chronological order) to show the most recent trace first.

Information on the Saved Trace List

The list provides information about the trace, including:

- Save start date
- Save start time
- Save end time
- Save user ID
- A short description of the trace
- Packet count
- Number of IP addresses within the trace

  If there are more IP addresses within this trace than can be incorporated into the IPFILE packet trace header record, a > symbol is displayed beside that IP address count to indicate this.
- The most common IP addresses
- A complete list of IP addresses, if you select a particular trace

For details of the information displayed and actions available, press F1 (Help).

Updating Packet Trace Description

The Packet Trace Description Update panel allows you to update the short description of the saved trace displayed on the Saved Trace List.

To access this panel, enter **U** (Update) beside an entry on the Saved Traced List.

The Packet Trace Description Update panel also displays key information from the Saved Trace List about the trace:

- Saved date and time
- User ID
- IP address count
- Packet count

Listing IP Addresses Within a Trace

The Packet Trace IP Address List displays a number of IP addresses (sorted in chronological order) within a selected trace. The number of IP addresses listed is the number of IP addresses that can be stored in the packet trace header record. If there are more IP addresses than those listed, a > symbol is displayed beside that IP address count on the Saved Trace List to indicate this.

To access this panel, enter **S/I** (IP Address List) beside an entry on the Saved Traced List.

```
PROD--------------- TCP/IP : Packet Trace IP Address List ---------------------
Command ===>                                                  Scroll ===> CSR

Trace Save Date & Time ... 04-AUG-2001 11:35:55  Saved By ... USER01
Short Description ........
                                                 S/C=Connection List P=Packet List
                           Connect  Packet  -------- First Occurrence --------
    IP Address        Bytes  Count   Count  Packet Date        Time
    123.0.77.22       51.75K    24     180       1 04-AUG-2001 11:35:16.721223
    123.183.123.128   3.710K     1      13       1 04-AUG-2001 11:35:16.721223
    123.0.91.167      11.21K     1      20       2 04-AUG-2001 11:35:16.731208
    123.123.10.33        552     0       6       4 04-AUG-2001 11:35:16.834914
    123.123.10.18     1.620K     1       4       8 04-AUG-2001 11:35:16.874008
    123.0.20.86          276     0       3      13 04-AUG-2001 11:35:16.926013
    123.0.0.10           300     0       5      14 04-AUG-2001 11:35:17.230040
    123.0.77.30          352     1       6      14 04-AUG-2001 11:35:17.230040
    123.0.123.192     1.018K     2       6      15 04-AUG-2001 11:35:17.254585
    123.0.123.191     1.018K     2       6      16 04-AUG-2001 11:35:17.262093
    123.0.123.193        363     3       9      23 04-AUG-2001 11:35:18.091432
    123.123.192.192       52     1       1      30 04-AUG-2001 11:35:18.194359
    123.0.91.101      3.405K     1      16      31 04-AUG-2001 11:35:18.507738
    123.11.215.2      16.45K     2      94      33 04-AUG-2001 11:35:19.153792
```

You can access a connection list or a packet list from this panel.

To change the sort order of IP addresses on the list, use the SORT command. To locate a specific IP address, use the LOCATE command.

Sorting IP Addresses

The SORT command allows you to display the Packet Trace IP Address List in a sort order other than the default chronological order.

The operand values for the command are associated with the column heading of the column you wish to sort by. For example, enter **SORT BYTES** to sort the list by the number of bytes.

SORT Operands

The SORT operands are:

?—Display the available sort values for the list.

IPADDR—Sort by IP addresses.

BYTES—Sort by the number of bytes in all packets for the address.

PKTCOUNT—Sort by the number or frequency of packets for the address.

TIME—Sort by time of first occurrence of a packet for the address in the trace.

To sort the list, do this:

1. At the Command ===> prompt, enter **SORT ?**. The Sort Values List is displayed, allowing you to select any of the listed values.
2. Select the sort value you want and press ENTER. The Packet Trace IP Address List is displayed sorted in the specified order.

Note: Alternatively, to change the sort order, issue the SORT *xxx* command (where *xxx* is a valid name, for a sort field, that consists of the minimum number of characters (for uniqueness) from the sort column heading).

For example, to sort by number of bytes, issue the SORT B command.

Locating IP Addresses

You can use the LOCATE command to position a particular row at the top of the list.

This command is available only when the IP address list has been sorted by use of the SORT command to change the default sort order (see the section “Sorting IP Addresses”).

The value you specify after the LOCATE command applies to the sort value that has been issued on the list. It does not necessarily apply to the first column of the list unless you have sorted by the first column.

Example

If you have sorted by time (the default sort order), and you issue the L 11:25:00 command, you are positioned at (the line before) the first time that starts with 11:25:00.

Actions on the Packet Trace IP Address List

S/C (Connection List)—Display a selection list (sorted into chronological order) of all connections found within the trace for the selected IP address.

P (Packet List)—Display a selection list (sorted into chronological order) of all packets found within the trace for the selected IP address.

Listing Connections Within a Trace

The Packet Trace Connection List displays connections (sorted into chronological order) within a selected trace. If optionally filtered for a specific IP address, all connections within the trace are listed.

This list has a header that displays some trace record information.

To access this panel, enter **C** (Connection List) beside an entry on the Saved Traced List or the Packet Trace IP Address List.

```
PROD--------------- TCP/IP : Packet Trace Connection List ---------------------
Command ===>                                                 Scroll ===> CSR

Trace Save Date & Time ... 04-AUG-1998 11:35:55  Saved By ... USER02
Short Description ........
                                                              S/P=Packet List
    ------------ Connection Details ------------ Packet        Time of First
    Foreign Host    FPort  Local Host      LPort  Count  Bytes Occurrence
    123.183.154.128  1032  123.0.77.55        23     13 3.710K 11:35:16.721223
    123.0.91.167     1037  123.0.77.55        23     20 11.21K 11:35:16.731208
    123.123.10.18    5406  123.0.77.55      2613      4 1.620K 11:35:16.874008
    123.0.123.192    4973  123.0.77.55      3776      4    959 11:35:17.254585
    123.0.123.191    4194  123.0.77.55      3776      4    959 11:35:17.262093
    123.0.123.193    1980  123.0.77.55      1974      5    203 11:35:18.091432
    123.0.123.193    1979  123.0.77.55      1975      2     80 11:35:18.110233
    123.0.77.30       520  123.123.192.192   520      1     52 11:35:18.194359
    123.0.91.101     1111  123.0.77.55        23     16 3.405K 11:35:18.507738
    123.0.91.203     1109  123.11.215.2      161     92 16.04K 11:35:19.153792
    123.11.215.2     1109  123.0.91.203      161     92 16.04K 11:35:19.153792
    123.0.91.165     1033  123.0.77.55        23     31    15K 11:35:19.468559
    123.0.77.27       520  123.0.77.55       520      2    104 11:35:19.946275
    123.0.77.22       520  123.0.77.27       520      2    104 11:35:19.946275
```

You can access a packet list from this panel; see the section “Listing Packets in a Selected Trace”).

To change the sort order of connections on the list, use the SORT command. To locate a specific connection, use the LOCATE command.

Sorting Connections

The SORT command allows you to display the Packet Trace Connection List in a sort order other than the default order of date and time.

The operand values for the command are associated with the column heading of the column (except the Connect Count column) that you wish to sort by. For example, enter **SORT BYTES** to sort the list by the number of bytes.

SORT Operands

The SORT operands are:

?—Display the available sort values for the list.

FHOST—Sort by IP addresses of the foreign hosts.

FPORT—Sort by port numbers of foreign ports.

LHOST—Sort by IP addresses of the local hosts.

LPORT—Sort by port numbers of local ports.

BYTES—Sort by the number of bytes in a packet.

PKTCOUNT—Sort by the number or frequency of packets.

TIME—Sort by time of first occurrence of the packet trace.

Locating Connections

You can use the LOCATE command to position a particular row at the top of the list.

This command is available only when the connection list has been sorted by use of the SORT command to change the default sort order (see the section “Sorting Connections”).

The value you specify after the LOCATE command applies to the sort value that has been issued on the list. It does not necessarily apply to the first column of the list unless you have sorted by the first column.

Action on the Packet Trace Connection List

S/P=Packet List—Display the Packet List.

Listing Packets in a Selected Trace

The Packet List displays all packets (sorted into chronological order) within a selected trace, optionally filtered for a specific IP address or connection. This list has a header that displays some trace record information.

To list the packets in a trace, enter **P** (Packet List) beside the trace that you want to view (if you just saved it, then it is at the top of the list) on the Saved Trace List.

Note: You can also display the Packet List from the following panels:

- The Packet Trace IP Address List, by entering **P** next to an IP address
- The Packet Trace Connection List, by entering **P** or **S** next to a connection

TCP/IP : Packet List (Parts 1,2, and 3)

```
PROD---------------------- TCP/IP : Packet List -----------------------------
Command ===>                                                 Scroll ===> PAGE

First Packet Date & Time ... 04-AUG-2001 11:35:16.731208
Short Description ..........
Local IP Address ........... 123.0.77.25      Local Port ..... 23
Foreign IP Address ......... 123.0.91.167     Foreign Port ... 1037
                                                                 S/F=Format
    Pos.In  --- Foreign Host ----     ---- Local Host -----    Time
     Trace  IP Address       Port Dir IP Address       Port   Diff  Bytes Prot
         2  123.0.91.167     1037 <<  123.0.77.25        23      - 1.464K  TCP
         3  123.0.91.167     1037 <<  123.0.77.25        23  <0.01 1.464K  TCP
        18  123.0.91.167     1037  >> 123.0.77.25        23   0.66     40  TCP
        19  123.0.91.167     1037 <<  123.0.77.25        23  <0.01    395  TCP
        22  123.0.91.167     1037  >> 123.0.77.25        23   0.57     40  TCP
        55  123.0.91.167     1037  >> 123.0.77.25        23   2.42     45  TCP
        56  123.0.91.167     1037 <<  123.0.77.25        23  <0.01     40  TCP
------------------------------------------------------------------------------
                                                                 S/F=Format
    Pos.In
     Trace  Dir Summary Information
         2  <<  Window: 1990   Flags: ACK PSH
         3  <<  Window: 1990   Flags: ACK PSH
        18   >> Window: 8760   Flags: ACK
        19  <<  Window: 1990   Flags: ACK PSH
        22   >> Window: 8405   Flags: ACK
        55   >> Window: 8405   Flags: ACK PSH
        56  <<  Window: 1985   Flags: ACK
------------------------------------------------------------------------------
                                                                 S/F=Format
    Pos.In  Occurred    Occurred   Elapsed
     Trace  Date        Time          Time Link            Via IP Address
         2  04-AUG-1998 11:35:16.73   0.00 OSATR0          123.0.77.26
         3  04-AUG-1998 11:35:16.73   0.00 OSATR0          123.0.77.26
        18  04-AUG-1998 11:35:17.39   0.66 OSATR0
        19  04-AUG-1998 11:35:17.39   0.66 OSATR0          123.0.77.26
        22  04-AUG-1998 11:35:17.97   1.24 OSATR0
        55  04-AUG-1998 11:35:20.40   3.67 OSATR0
        56  04-AUG-1998 11:35:20.40   3.67 OSATR0          123.0.77.26
```

The Packet List shows details of the packets that were traced.

If the save processing found major errors (such as missing records or invalid packet headers) when reading packets from the CTRACE file, then the corresponding entries are displayed in red.

To view different types of information on the Packet List, you can scroll in any of the following ways:

- Scroll right (F11) to view summary information about each packet on the list. See part 2 of the previous figure for information resulting from packet analysis.
- Scroll right (F11) again to view date, time, and link information.
- Scroll left (F10) to return to a previous part of the Packet List.

For details of the information displayed and actions available, press F1 (Help).

Viewing Data for a Selected Packet

To view the contents of a packet from the Packet List, enter **F** (Format) or **S** (Select) beside the packet that you want to view. The Formatted Packet Display is presented.

The contents of the Formatted Packet Display vary according to the type of packet and its contents.

TCP/IP : Formatted Packet Display (Format A)

```
PROD------------------ TCP/IP : Formatted Packet Display -------Columns 001 079
Command ===>                                                    Scroll ===> PAGE

******************************** TOP OF DATA ********************************
PKT  Packet # ..... 00000002     Direction .........  Recv
     Date ......... 19-SEP-2001  Time ..............  10:16:58.408203
     Link Name .... OSATR0       Device Type .......  LCS_TOKEN_RING

IP   Source Addr ..... 123.0.91.126    Destination Addr ... 123.0.77.25
     IP Version ...... 4                Header Length ...... 5
     Type of Service . B'00000000'      Total Length ....... 40
     Identification .. 47203            Flags .............. B'010'
     Frag Offset ..... 0                Time To Live ....... 125
     Protocol ........ TCP              Header Chksum ...... X'0BD4'

TCP  Src Port ........ 2336             Dest Port ... TELNET
     Seq Number ...... X'F9F3F6F5'      Ack Number .. X'F6F8F3F4'
     Data Offset ..... 20               Flags ....... ACK
     Window .......... 8638             Checksum .... X'C06C'
     Urgent Pointer .. 0

          +----------- TCP Data ------------+ +--- EBCDIC ---+ +---  ASCII ---+
```

There are three display formats for the Formatted Packet Display (see the following figures for format B and format C). You can move between the three display formats by pressing F6 (Format).

You can scroll up (F7) and down (F8) for more information about this packet, and you can use F10 and F11 to display the details of the previous or next packet respectively.

You can use the PRINT command to print the information displayed on the panel.

For more details of the data shown on these display formats, see the section "Viewing the Formatted Packet Display ".

For more information about the information displayed, see the *Request for Comments* (RFC) for the protocol being used:

- *RFC 791* for IP
- *RFC 793* for TCP
- *RFC 768* for UDP
- *RFC 792* for ICMP

Currently the following Web sites have RFC documentation online:

- http://www.faqs.org/rfcs/
- http://www.freesoft.org/CIE/index.htm
- http://www.ietf.org/rfc.html

TCP/IP : Formatted Packet Display (Format B)

```
PROD------------------ TCP/IP : Formatted Packet Display -------Columns 001 079
Command ===>                                                    Scroll ===> PAGE

******************************** TOP OF DATA *********************************
PKT  Packet # ..... 00000002     Direction .........  Recv
     Date ......... 19-SEP-2001  Time ..............  10:16:58.408203
     Link Name .... OSATR0       Device Type .......  LCS_TOKEN_RING

IP   Source Addr ..... 123.0.91.126    Destination Addr ... 123.0.77.25
     IP Version ...... 4               Header Length ...... 5
     Type of Service . B'00000000'     Total Length ....... 40
     Identification .. 47203           Flags .............. B'010'
     Frag Offset ..... 0               Time To Live ....... 125
     Protocol ........ TCP             Header Chksum ...... X'0BD4'

          +----------- IP Header -----------+ +--- EBCDIC ---+ +---  ASCII ---+
    +0000 45000028 B8634000 7D060BD4 C7005B7E         '  MG $= E  ( c@ }      ~
    +0010 C7005019                              G &               P

TCP  Src Port ........ 2336           Dest Port ... TELNET
     Seq Number ...... X'F9F3F6F5'    Ack Number .. X'F6F8F3F4'
     Data Offset ..... 20             Flags ....... ACK
```

TCP/IP : Formatted Packet Display (Format C)

```
******************************** TOP OF DATA ********************************
PKT  Packet # ..... 00000002     Direction .........  Recv
     Date ......... 19-SEP-2001  Time ..............  10:16:58.408203
     Link Name .... OSATR0       Device Type .......  LCS_TOKEN_RING


          +-------- IP Header Data ---------+ +--- EBCDIC ---+ +---  ASCII ---+
     +0000 45000028 B8634000 7D060BD4 C7005B7E          '  MG $= E  ( c@ }      ~
     +0010 C7005019                          G &               P


          +------------ IP Data ------------+ +--- EBCDIC ---+ +---  ASCII ---+
     +0000 09200017 28BCF407 37D33643 501021BE       4  L  &        (   7 6CP !
     +0010 C06C0000                          {%               l
****************************** BOTTOM OF DATA ******************************
```

Viewing the Formatted Packet Display

There are several groups of data displayed on the Formatted Packet Display. Some of these groups of data are displayed on only one format of the panel; others are displayed on two or three of the formats.

Each group of data relates to one of the following:

- The packet as a whole
- IP
- The related protocol (TCP, UDP, or ICMP)

The groups of data displayed in the different formats are:

Format	Data Displayed
A	Packet details IP header fields IP options Protocol header fields Protocol data
B	Packet details IP header fields IP options IP header Protocol header fields Protocol header data Protocol data
C	Packet details IP header IP data

Packet Details on the Formatted Packet Display

Packet details are displayed on all three formats of the Formatted Packet Display.

Packet Details on the Formatted Packet Display

```
PKT  Packet # ........ 00000002        Direction .........  Send
     Date ............ 12-Mar-2001     Time ..............  15:32:09.456064
     Link Name ....... IUCVLNK         Device Type .......  IUCV
     Via Addr ........ 192.0.77.55
```

For more information about packet details, press F1 (Help).

IP Header Fields on the Formatted Packet Display

IP header fields for the packet are displayed on formats A and B of the Formatted Packet Display.

IP Header Fields on the Formatted Packet Display

```
     IP Version ...... 4               Header Length ...... 5
     Type of Service . B'00000000'     Total Length ....... 472
     Identification .. 22900           Flags .............. B'000'
     Frag Offset ..... 0               Time To Live ....... 60
     Protocol ........ UDP             Header Chksum ...... X'D555'
```

For more information about the fields, press F1 (Help).

IP Options on the Formatted Packet Display

For some packets, there is a group of items displayed as IP options on format A of the Formatted Packet Display.

IP Options on the Formatted Packet Display

```
     OPTION=COPY   CONTROL  LOOSE_SRC LEN=11 PTR=4
           1.2.3.4
           5.6.7.8
     OPTION=NOCOPY CONTROL  END_LIST
```

For more information about IP options, see *RFC 791*.

Protocol Header Fields on the Formatted Packet Display

Protocol header fields are displayed on formats A and B of the Formatted Packet Display. The header displayed depends on the protocol: TCP, UDP, or ICMP.

TCP Header Fields on the Formatted Packet Display

```
TCP  Src Port ........ TELNET          Dest Port ... 3355
     Seq Number ...... X'F9F3F6F5'     Ack Number .. X'F6F8F3F4'
     Data Offset ..... 20              Flags ....... ACK PSH
     Window .......... 1853            Checksum .... X'6981'
     Urgent Pointer .. 0
```

For more information about the fields, press F1 (Help).

UDP Header Fields on the Formatted Packet Display

```
UDP  Src Port ........ 53              Dest Port ... 1173
     Length .......... 94              Checksum .... X'BE47'
```

For more information about the fields, press F1 (Help).

ICMP Header Fields on the Formatted Packet Display

```
ICMP Msg Type ............... Echo Request
     Code ................... 0
     Checksum ............... X'7A94'
     Identifier ............. 12
     Sequence Number ........ 0
```

For more information about the fields, press F1 (Help).

TCP Options on the Formatted Packet Display

For some packets, there is a group of items displayed as TCP options on format A of the Formatted Packet Display.

TCP Options on the Formatted Packet Display

```
 TCP Option              Value
 ----------              -----
 Maximum Segment Size    255
 No Operation
 End Of Options List
```

For more information about TCP options, see *RFC 793*.

Protocol Data on the Formatted Packet Display

Protocol data is displayed on formats A and B of the Formatted Packet Display. Protocol header data is displayed on format B only.

The details displayed depend on the protocol: TCP, UDP, or ICMP.

TCP Data on the Formatted Packet Display

```
      +----------- TCP Data ------------+ +--- EBCDIC ---+ +---  ASCII ---+
+0000 3C404000 13114040 2902C0E8 42F5E2E3           {Y 5ST <@@   @@)   B
+0010 D5D4F13C 40616029 02C0E842 F5E2A385 AB1  /-  {Y 5Abc     <@a)   B
+0020 8740E296 12A3A456 12345678 C0E842F5 g Software  {Y 5  @        )   B
+0030 3CC15060 11C15029 02C0E842 F23CC260  A&- A&  {Y 2 B- < P P)   B <
+0040 4011C260 2902C0F0 42F43CC2 E6402902   B-  {0 4 BW    @  )   B <  @)
+0050 C0E842F7 4E3CC27D 604E3CC3 12345678 {Y 7+ B'-+ C-      B N< }< @)
+0060 C0F042F4 D3E44040 12345678 C0E842F7 {0 4LU      {Y 7   B   @@@@)   B
+0070 D5D5D5D5 D5F0F0F2 11C3F029 02C0F042 aaaaa002 C0  {0              )   B
+0080 F43CC3F6 402902C0 E842F74F 3CC4C67E 4 C6   {Y 7| DF=  <  @)   B O<  ~
+0090 3CC44D40 4F3CC4D6 402902C0 F042F1D6  D( | DO   {0 1O < M@O<  @)   B
+00A0 2902C0E8 42F7D629 02C0E842 F2D62902   {Y 7O  {Y 2O   )   B  )   B  )
```

TCP Data—The packet's TCP data, displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

TCP Header Data on the Formatted Packet Display

```
      +-------- TCP Header Data --------+ +--- EBCDIC ---+ +---  ASCII ---+
+0000 00170D1B 0DBC6D44 0DA807C4 5018073D       _  y D&          mD    P  =
+0010 69810000                           a              i

TCP Header Data—The packet's TCP header data, displayed in three columns in
different representations: hexadecimal, EBCDIC, and ASCII.
```

UDP Data on the Formatted Packet Display

```
      +----------- UDP Data ------------+ +--- EBCDIC ---+ +---  ASCII ---+
+0000 00018580 00010001 00000000 02353302   e                          53
+0010 12345678 12345678 07696E2D 61646472           > /    90 0 192 in-addr
+0020 04617270 6100000C 0001C00C 000C0001  /  /     {       arpa
+0030 0000D141 12345678 616E796D 65646502   J     />_        A   ganymede
+0040 12345678 03313939 07696E2D 61646472           > /    90 0 192 in-addr
+0050 04617270 6100                       /  /             arpa
```

UDP Data—The packet's UDP data, displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

UDP Header Data on the Formatted Packet Display

```
      +---------- UDP Header -----------+ +--- EBCDIC ---+ +---  ASCII ---+
+0000 00350495 005EBE47                     n ;            5    G
```

UDP Header Data—The packet's UDP header data, displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

ICMP Data on the Formatted Packet Display

```
          +----------- ICMP Data -----------+ +--- EBCDIC ---+ +---  ASCII ---+
    +0000 48B63B8B 1A1F56FF 10111213 14151617                  H ;   V
    +0010 18191A1B 1C1D1E1F 20212223 24252627                        !"#$%&'
    +0020 28292A2B 2C2D2E2F 30313233 34353637                  ()*+,-./01234567
    +0030 38393A3B 3C3D3E3F 40414243 44454647                  89:;<=>?@ABCDEFG
    +0040 48494A4B 4C4D4E4F 50515253 54555657   ¢.<(+|&        HIJKLMNOPQRSTUVW
    +0050 58595A5B 5C5D5E5F 60616263 64656667   !$*);-/       XYZ  _
    +0060 68696A6B 6C6D6E6F 70717273 74757677   <x:ad>,%_>?
hijklmnopqrstuvw
    +0070 78797A7B 7C7D7E7F 80818283 84858687  :#@'=" abcdefg xyz{<x:ad>}~
    +0080 88898A8B 8C8D8E8F 90919293 94959697 hi       jklmnop
    +0090 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 qr       ~stuvwx
    +00A0 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 yz
```

ICMP Data—The packet's ICMP data, displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

ICMP Header Data on the Formatted Packet Display

```
          +---------- ICMP Header ----------+ +--- EBCDIC ---+ +---  ASCII ---+
    +0000 08007A94 000C0000                   :m              z
```

ICMP Header Data—The packet's ICMP header data, displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

IP Data on the Formatted Packet Display

```
          +------------ IP Data ------------+ +--- EBCDIC ---+ +---  ASCII ---+
    +0000 00170D1B 0DBC6D44 0DA807C4 5018073D       _  y D&          mD    P  =
    +0010 12345678 01C21140 40290142 F4114040  a   B      4    i      @@) B  @@
    +0020 3C404000 12345678 2902C0E8 42F5E2E3           {Y 5ST <@@   @@)   B
    +0030 D5D4F13C 12345678 02C0E842 F5E2A385 XX1  /-  {Y 5Abc    <@a)   B
    +0040 12345678 8740E296 86A3A681 12345678 defgh Software        @        )
    +0050 C0E842F5 3CC15060 11C15029 02C0E842 {Y 5 A&- A&  {Y    B < P P)   B
    +0060 F23CC260 4011C260 2902C0F0 42F43CC2 2 B-  B-  {0 4 B  < @  )   B <
    +0070 E6402902 C0E842F7 4E3CC27D 604E3CC3 W   {Y 7+ B'-+ C  @)   B N< }<
    +0080 60402902 C0F042F4 D3E44040 40402902 -   {0 4LU       @)   B   @@@@)
    +0090 C1E234F5 D5D5D5D5 D5F0F0F2 11C3F029 {Y 7aaaaa002 C0    B            )
    +00A0 02C0F042 F43CC3F6 402902C0 E842F74F  {0 4 C6   {Y 7|    B <  @)   B O
```

IP Data—The packet's IP data, displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

IP Header Data on the Formatted Packet Display

```
         +----------- IP Header -----------+ +--- EBCDIC ---+ +---  ASCII ---+
    +0000 450004D8 721C0000 3C06A9AB C7005019    Q      z G &  E   r   <     P
    +0010 C700803E                            G                 >
```

IP Header—The packet's IP header data, displayed in three columns in different representations: hexadecimal, EBCDIC, and ASCII.

Printing Formatted Packet Details

You can use the PRINT command to print the formatted packet.

A confirmation panel is displayed, prompting you for printer details.

Errors in Packets

Sometimes during the formatting of a packet trace errors are found, such as invalid field values in packet headers. The Packet Trace facility displays warning messages, in red, on the Formatted Packet Display panels to inform you of these errors.

The warning messages relate to such things as:

- Incorrect lengths
- Invalid use of flags
- Invalid field values
- Reserved fields being used
- Invalid IP and TCP options
- Invalid checksums

```
PROD------------------ TCP/IP : Formatted Packet Display -------Columns 001 079
Command ===>                                                    Scroll ===> CSR

******************************** TOP OF DATA ********************************
PKT  Packet # ..... 00000001     Direction .........  Send
     Date ......... 23-SEP-2001  Time ..............  15:46:54.135244
     Link Name .... OSAPORT      Device Type .......  LCS_TOKEN_RING
     Via Addr ..... 123.0.77.26

IP   Source Addr ..... 123.0.77.55     Destination Addr ... 123.0.128.62
     IP Version ...... 4               Header Length ...... 6
     Type of Service . B'00000000'     Total Length ....... 48
     Identification .. 29212           Flags .............. B'000'
     Frag Offset ..... 0               Time To Live ....... 60
     Protocol ........ TCP             Header Chksum ...... X'9BC7'
     *WARNING* Invalid IP Checksum. Expected X'AC53'. Found X'9BC7'
```

Dealing with Errors in Packets

If there are warnings of errors in the traced packets, do the following:

- Read the appropriate *Request for Comment* (RFC) to determine the correct usage of fields in the protocol. For information about locating RFCs, see the section “IP Options on the Formatted Packet Display”).
- Identify the device / program that is sending the invalid packets.
- Identify other IP devices that the packet traversed, as they may be corrupting the packet.
- Rectify the problem.

Chapter 21

Connecting to Remote Hosts by Using Telnet

This chapter contains the following topics:

- Using Telnet to Connect to Remote Hosts
- Starting Telnet Connections
- Managing Your Telnet Connection
- Ending Your Telnet Connection
- Using Line Commands to Connect to a Remote Host
- Sending Control Codes or Special Characters to the Remote Host

Using Telnet to Connect to Remote Hosts

The Telnet protocol can be used to:

- Connect to remote hosts (this could be a channel card, a router, or a UNIX system).
- Connect to network management platforms from where you can issue commands.

For example, you might want to view the status of a router's interfaces, or update its configuration.

By using NetMaster for TCP/IP, you can establish a Telnet connection to a remote host in the following modes:

- Full screen mode
- OCS takeover mode
- Line mode

Connecting in Full Screen Mode

Full screen mode uses a full screen of the 3270 to display the Telnet connection line by line. The NetMaster for TCP/IP Telnet function supports simple line-by-line access to the remote system. It emulates a line-by-line terminal. The Telnet protocol calls this a network virtual terminal (NVT).

This support allows rapid problem diagnosis when used from other NetMaster for TCP/IP displays such as the traceroute display. The NetMaster for TCP/IP Telnet function does not provide access to remote facilities that use more advanced terminal facilities, for example, full-screen editors.

For a description of the full screen mode, see the section "Starting Telnet Connections".

Connecting in OCS Takeover Mode or Line Mode

When you start a Telnet connection in OCS takeover mode or line mode, you have the added benefit of being able to issue Telnet and Management Services commands from the same command entry point at the same time.

For a description of connecting to a host in OCS takeover mode or line mode, see the section "Using Line Commands to Connect to a Remote Host".

Starting Telnet Connections

To start a Telnet connection to a remote host, do the following:

1. Enter /IPDIAG at the ===> prompt. The Network Diagnosis Functions menu is displayed.
2. Select the **TN** - Start a Telnet Connection option.
3. Specify the name or IP address of the remote host to which you want to start a Telnet connection in the Host Name / Address field
4. Press ENTER. The TCP / IP : Telnet panel is displayed.

```
PROD---------------------- TCP/IP : Telnet 123.168.2.66 ------------Line 1 of 10
Command ===> User01
        ===>

Status Connected     Limit 1000   Wrap OFF   Edit OFF   Scroll OFF
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
TNVT0102 Telnet PROCESS 123.168.2.66 STARTED FOR HOST 123.168.2.66
TNVT0106 CONNECTING TO 123.168.2.66 ON PORT 23
TNVT0107 CONNECTED TO mercury.dept.company.com
TNVT0108 HOST ADDRESS 123.168.2.66 FULL NAME mercury.dept.company.com

ULTRIX V4.3A (Rev. 146) (mercury.dept.company.com)

login:
** END OF DELIVERED MESSAGES **
```

5. If required, type your login ID for the remote host at the command line and press ENTER. If necessary, repeat this procedure with your password.

   Note: If you do not want data entered on the command line (for example, your password) to be visible, press F5 (Hide) before typing.

```
PROD---------------------- TCP/IP : Telnet 123.168.2.66 ------------Line 1 of 10
Command ===> User01
        ===>

Status Connected     Limit 1000   Wrap OFF   Edit OFF   Scroll OFF
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
TNVT0102 Telnet PROCESS 123.168.2.66 STARTED FOR HOST 123.168.2.66
TNVT0106 CONNECTING TO 123.168.2.66 ON PORT 23
TNVT0107 CONNECTED TO mercury.dept.company.com
TNVT0108 HOST ADDRESS 123.168.2.66 FULL NAME mercury.dept.company.com

ULTRIX V4.3A (Rev. 146) (mercury.dept.company.com)

login:
** END OF DELIVERED MESSAGES **
--------------------------------------------------------------------------------
Status Connected     Limit 1000   Wrap OFF   Edit OFF   Scroll OFF
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
Last login: Tue Apr  2 11:58:51 from testmvs01.dept.company.com
ULTRIX V4.3A (Rev. 146) System #3: Mon Feb 14 12:05:02 EST 1934
UWS V4.3A (Rev. 25)

               CompanyName Corporation
               Corporateville, State

Tue Apr  2 12:16:01 EST 1936
mercury.dept.company.com>
** END OF DELIVERED MESSAGES **
```

Other Methods of Starting Full Screen Telnet Connections

You can also start a full screen (FS) Telnet connection as follows:

- By entering **TN** against a CIP or router resource on the IP resource monitor
- By entering **TN** against a node on the IP node monitor
- By applying the **TN** (Telnet) action against a host or router on the Trace Route Result List
- By applying the **TN** (Telnet) action against a router on the Routing Table
- From an OCS window by using the command:

  ```
  TELNET host_name|IP_address MODE=FS
  ```

- By pressing F4 (Telnet) from many panels such as channel card and 2216 router panels.

About the Telnet Display

From the Telnet display, you can issue commands and pass data to the remote host to which the connection has been made—the IP address or host name of this connection is displayed in the title line.

All data resulting from any processing you do on the remote host is held in a buffer. The size of the buffer and the number of the first line displayed are shown on the right portion of the title line. You can move around the data held in this buffer by using the following function keys that support the standard NetMaster for TCP/IP scrolling commands:

- F7 (Backward)
- F8 (Forward)
- F10 (Left)
- F11 (Right)

Note: Commands entered in the command line of the Telnet display are sent directly for processing on the remote host.

Telnet Specific Function Key Assignments

The following is a description of each of the function key assignments exclusive to the Telnet display:

Function (F4)—Presents the Telnet Functions menu from where you can select the options to manage your Telnet connection

Hide (F5)—Suppresses the display of the characters being typed as you enter your password when logging on to a Telnet connection on a remote host—this also suppresses data from going into the command stack used by Retrieve (F6) as well as that resulting from tracing.

Retrieve (F6)—Retrieves previously issued commands from the command stack, starting with the most recent. When the cursor is positioned on a line in the display, then that line is retrieved.

By pressing Retrieve (F6) three times, you display a list of previously entered commands.

Fields on the Telnet Display

For details of the information displayed, press F1 (Help).

Editing Text on the Telnet Display

If you want to reformat the data on your Telnet display before printing it, or if you want to use particular data or messages as input—for example, to a problem record—ensure that the Edit field on the Telnet display is set to ON. When Edit is set to ON, the display is presented in Edit mode. This is an ISPF-like interface and supports most of the standard ISPF editing commands.

Some simple editing commands are as follow:

- **D** or **DD** (Delete)—to delete one line of text, type the **D** command in the first column to the left on the line you want to remove and press ENTER. To delete more than one line, enter **DD** at the first and last lines of the block you want to remove.
- **N** or **NN** (Notepad)—to copy one line of text to the Notepad, type the **N** command in the first column to the left on the line you want to copy to the Notepad and press ENTER. To copy more than one line, enter **NN** at the first and last lines of the block you want to copy.

For further information about editing your Telnet display, see the *Managed Object Development Services Programming and Administration Guide.*

```
PROD---------------------- TCP/IP : Telnet 123.168.2.66 ----------Line 10 of 35
Command ===>
        ===>

Status Connected     Limit 1000   Wrap OFF   Edit ON    Scroll OFF
LINE 1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---
0010 Password:
0011 Last login: Wed May  8 08:25:24 on :0
0012 ULTRIX V4.3A (Rev. 146) System #3: Mon Feb 14 12:05:02 EST 1994
0013 UWS V4.3A (Rev. 25)
NN14
0015                 CompanyName Corporation
NN16                 Corporateville, State
0017
0018 This display is now in full edit mode.
0019 Lines 14 to 16 of this display contain the NN (Notepad) command.
0020 When ENTER is pressed, these lines will be copied to the Notepad from
0021 where they can later be moved into a problem record for example, by using
0022 the QQ (Queue) command in the same way.
0023 If you want to move just one line of text use a single N instead of NN.
0024 If you want to remove lines of text from the display, use D or DD (Delete)
0025
```

Managing Your Telnet Connection

NetMaster for TCP/IP provides a number of useful functions to help you manage your Telnet connection.

To display the Functions menu, press F4 (Function).

```
PROD---------------------- TCP/IP : Telnet 123.168.2.66 -----------Line 13 of 26
Command ===>
        ===>

Status Connected     Limit 1000   Wrap OFF   Edit OFF   Scroll OFF
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----

Last login: Tue Apr  2 11:58:51 from testmvs1.dept.
ULTRIX V4.3A (Rev. 146) .- Functions -------------------.ST 1934
UWS V4.3A (Rev. 25)     |                               |
                        |  _  1. Find...                |
                Company |     2. Print...              |
                Corpora |     3. Options...            |
                        |     4. Telnet Commands...     |
                        |     5. Clear Buffer           |
                        |     6. Keys Off               |
                        |     7. Connection Details...  |
Tue Apr  2 12:16:01 EST |     8. Disconnect             |
mercury.dept.company.co |                               |
** END OF DELIVERED MES '-------------------------------'
```

The Telnet functions are as follows:

Find—specifies a string of text and search for it in the buffer.

Print—prints the contents of the buffer.

Options—sets up or alter your Telnet connection.

Telnet Commands—issues any of four standard Telnet commands.

Clear Buffer—Clears the buffer of all existing data.

Keys Off/On—Hides or shows the function key display.

Connection Details—Provides you with statistical information about the current connection.

Disconnect/Reconnect—Exits you from the current connection or, if currently disconnected, lets you reconnect.

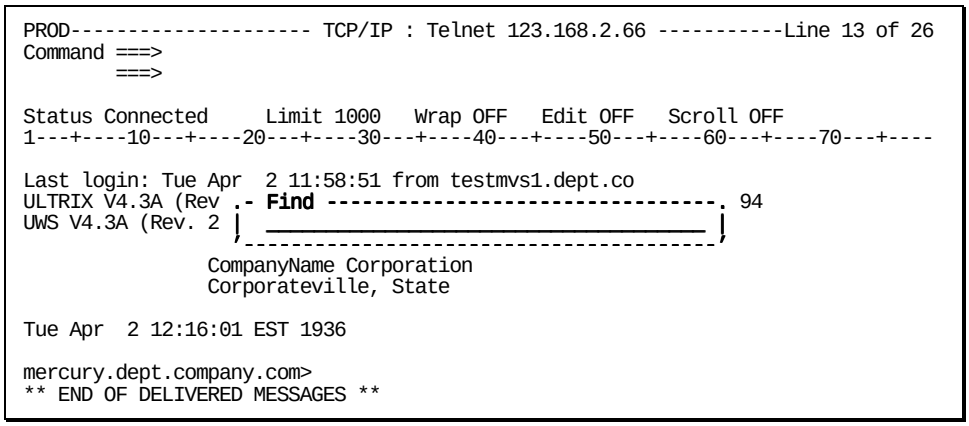
Each window displayed as a result of selecting a Telnet function from the Functions list has the following function key assignments:

F1	Help—display help for the window being displayed
F2	Split—create a second active window.
F3	Exit—terminate the current processing level and return control to the higher level.
F9	Swap—swap between the current window and another active window. If no other window is active, then one is created.

Searching Data on the Telnet Display

A search facility is provided to enable you to find occurrences of text that match a specified string. To find a particular text string in the buffer, do the following:

1. Enter **1** on the Functions menu. The Find window is displayed.



2. Specify the text string you want to find and press ENTER. The cursor is placed at the first character of the found text.
3. To locate further instances of the text string, continue to press ENTER—when there are no more instances of text that match the search string, a message is displayed informing you that the bottom of the data has been reached. Press ENTER again to return to the top of the data and continue the search.

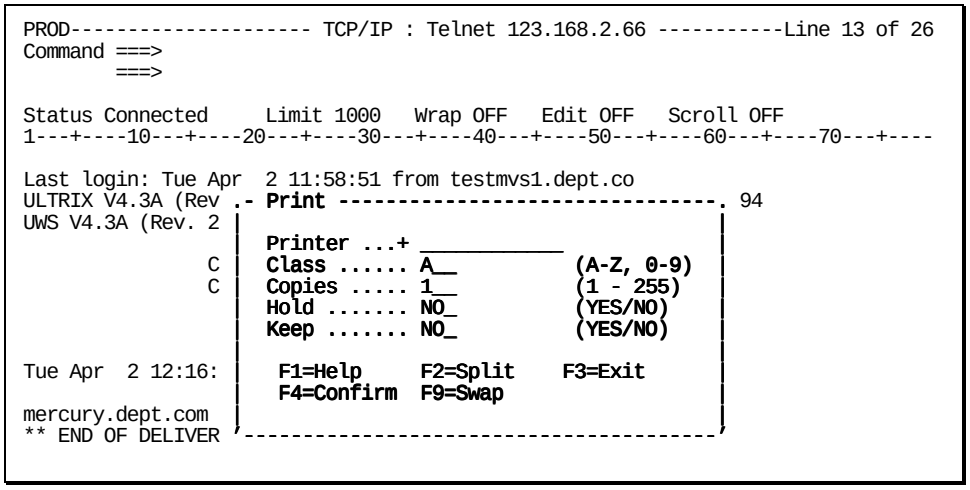
To close the Find window, press F3 (Exit). The last string entered in the Find window is retained and displayed the next time the Find function is used.

Printing from the Telnet Display

You can print the contents of the Telnet buffer to any printer defined in the Print Services Manager (PSM). (For information about PSM, see the *Management Services User's Guide*).

To print the contents of the Telnet buffer, do the following:

1. Enter **2** on the Functions menu. The Print window is displayed.



2. Enter the name of the printer to which you want to send the output.

   If you are unsure of the name of the printer, do the following:

   - Type **?** in the Printer field and press ENTER—the PSM : Printer List is displayed.
   - Select the printer you want to use and press ENTER—you are returned to the Print window, and the name of the printer is placed in the field.

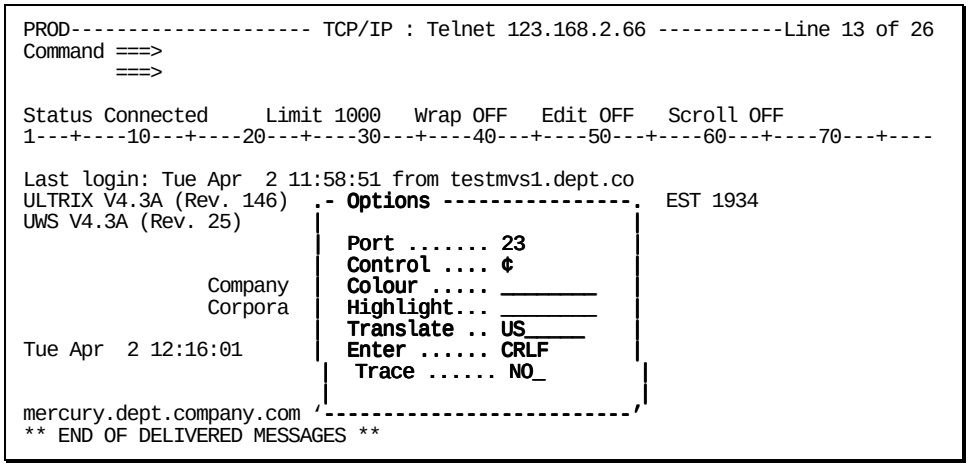
3. Enter the number of copies you want to produce.

4. Set the Hold value—use the default value of NO if you want to print the output immediately. Change it to YES if you want to hold the output on the spool to be printed later.
5. Set the Keep value—use the default value of NO if you want the print job removed from the spool immediately after printing. Change it to YES if you want to keep the output on the spool so that it may be reprinted later if required.
6. Press the Confirm key—depending on the value in the Hold field, the output is sent to the spool and either held in the queue, or printed immediately.

Setting Your Telnet Options

You can configure your Telnet connection to suit your particular requirements. To change the Telnet options, do the following:

1. Enter **3** on the Functions menu. The Options window is displayed.



2. Make any required changes and press ENTER to confirm the changes.

If you change any of the options while your Telnet display has a status of Disconnected, an attempt is made to reconnect you with the new options. If the attempted reconnect fails (for example, you might have specified an unsupported port), an appropriate message is displayed and the status of the Telnet display changes to Error.

Fields in the Telnet Options Window

For details of the information displayed, press F1 (Help).

Issuing Telnet Commands

A set of four standard Telnet commands is implemented with NetMaster for TCP/IP. When issued, these commands are sent to the remote host, which processes them accordingly. The following is a brief description of each of these commands:

Abort Output—Allows a process that is generating output to run to completion, but without sending the output to your terminal.

Are You There—Sends a request to provide visible evidence that this connection is still active; for example, this command might be used if the system has been unexpectedly *silent* for an extended period of time.

Break—Simulates a Break key or Attention key.

Interrupt Process—Suspends, interrupts, aborts, or terminates the process to which you are connected.

To issue any one of the above Telnet commands, do the following:

1. Enter **4** on the Functions menu. The CAS : Valid Value List for the Telnet Commands is displayed.
2. Select the Telnet command you want to issue and press ENTER. The command is issued.

```
PROD---------------------- CAS : Valid Value List ----------------------------4
Command ===>                                                  Scroll ===> PAGE

                                                            S/=Select (one only)
    Field: TELNET Command

    Full Value   Description
    AO           Abort Output
    AYT          Are You There
    BRK          Break
    IP           Interrupt Process
    **END**
```

Clearing the Buffer

To remove all of the data in the buffer, enter **5** on the Functions menu.

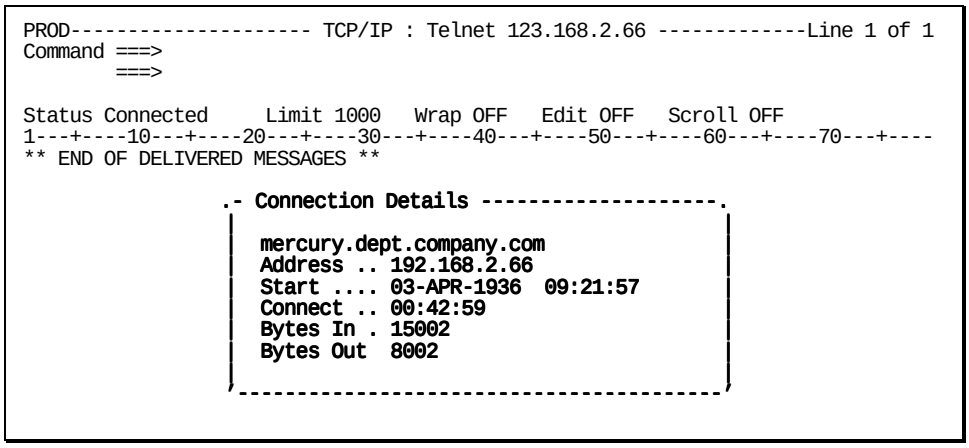
Hiding or Displaying the Function Key Assignments

If you want to hide the function key assignments that are displayed at the bottom of the Telnet panel, enter **6** on the Functions menu.

Alternatively, if the function key assignments are already hidden, this option appears in the Functions menu as Keys On and can be selected when you want them to be displayed.

Displaying Telnet Connection Details

If you want to display information pertaining to your current Telnet session, enter **7** on the Functions menu. The Connection Details window is displayed.



For details of the information displayed, press F1 (Help).

Ending Your Telnet Connection

The most direct way to end your session on the remote host and exit is to press F3 (Exit).

To end your session on the remote host and remain in the Telnet display, do the following:

1. Press F4 (Function). The list of functions is displayed.
2. Enter **8** on the Functions menu. The session is ended and the Status field now contains the value of Disconnected.

This function is useful if you want to change any of your connection's option settings, while retaining access to the Telnet display and its Functions menu after disconnecting.

```
PROD--------------------- TCP/IP : Telnet 123.168.2.66 -----------Line 13 of 26
Command ===>
        ===>

Status Connected     Limit 1000   Wrap OFF   Edit OFF   Scroll OFF
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----

Last login: Tue Apr  2 11:58:51 from testmvs1.dept.co
ULTRIX V4.3A (Rev. 146) .- Functions -------------------. ST 1934
UWS V4.3A (Rev. 25)     |                               |
                        |  8  1. Find...                |
                Company |     2. Print...              |
                Corpora |     3. Set Options...         |
                        |     4. Telnet Commands...     |
                        |     5. Clear Buffer           |
                        |     6. Keys Off               |
Tue Apr  2 12:16:01     |     7. Connection Details...  |
                        |     8. Disconnect             |
                        |                               |
mercury.dept.company.co '-------------------------------'
 ** END OF DELIVERED MESSAGES **
-------------------------------------------------------------------------------
PROD--------------------- TCP/IP : Telnet 192.168.2.66 -------------Line 1 of 3
Command ===>
        ===>
Disconnect request accepted
Status Disconnected  Limit 1000   Wrap OFF   Edit OFF   Scroll OFF
1---+----10---+----20---+----30---+----40---+----50---+----60---+----70---+----
TNVT0109 SESSION DISCONNECTED BY USER REQUEST
TNVT0105 Telnet SESSION ID=192.168.2.66 ENDED,CONNECT TIME 0 Hours 28 Minutes 1
** END OF DELIVERED MESSAGES **
```

If you want to re-establish a connection with the remote host, press F4 (Function) and enter **8**. A connection is made with the remote host and you are prompted for your login ID and password.

Using Line Commands to Connect to a Remote Host

A benefit of using the TELNET command to establish a connection from an OCS window or from the Command Entry panel is that you can issue both Telnet and Management Services commands from the same command entry point at the same time.

The TELNET command can be used in the following ways:

- OCS takeover mode
- Line mode
- As part of an NCL procedure

Regardless of the way in which you use the TELNET command to establish a connection, you might need to occasionally send special characters to the remote host. For information about sending control codes and special characters to the remote host, see the section “Sending Control Codes or Special Characters to the Remote Host”.

Starting a Telnet Connection

To start a Telnet connection, use the following command form:

TELNET *ip_address* | *host_name*

To start a connection with a configuration other than the default (for example, to connect to the remote host *mercury* on a port other than the default port 23), you should enter the command as follows:

TELNET *mercury* PORT=1976

See the *Management Services Command Reference* for the syntax of the TELNET command and a description of each of its operands.

Using Telnet in OCS Takeover Mode

You can turn your OCS window into a virtual terminal for a nominated remote host by using the OCS takeover mode. In takeover mode, you retain the ability to issue Management Services commands and receive unsolicited notifications, but you can also issue commands directly to the remote host by typing the command and pressing ENTER.

To start a Telnet connection to the remote host, *mercury*, in takeover mode, use the TELNET command in the following form:

TELNET *mercury* MODE=OCS

Note: MODE=OCS is the default when you are in OCS.

When you establish a connection in OCS takeover mode, the name of the remote host to which you are connected is displayed to the right on the line immediately above the command entry line.

```
(11.45)------------ NetMaster Operator Console Services ----------------------

Tue Apr  9 11:45:41 EST 1936

mercury.dept.company.com>
_____________________________________________________________________________
login:
user01

Password:

Last login: Tue Apr  9 10:56:31 from testmvs01.dept.co

ULTRIX V4.3A (Rev. 146) System #3: Mon Feb 14 12:05:02 EST 1934
UWS V4.3A (Rev. 25)

                CompanyName Corporation
                Corporateville, State

------------------------------- NetMaster --------------------------- mercury
==>
```

When you press the ENTER key in takeover mode, the data you have entered at the command line is passed to the remote host—to enter Management Services commands, type the command and press F12. When you start a Telnet connection in takeover mode it overrides the following function key assignments in your OCS window:

F3	Becomes Disconnect—this is used to end your current Telnet connection and reinstate normal function key assignments.
F12	Becomes the OCS Enter key—this is used to issue Management Services commands in the OCS environment.
ENTER	Becomes the Telnet Enter key—this is used to issue commands to the remote host.

Using Telnet in Line Mode

In line mode, you retain normal OCS operation and must issue a new command each time you want to communicate with the host.

As an example, to start a Telnet connection to the host, *mercury*, in line mode, use the following command form:

```
TELNET mercury MODE=LINE
```

To send data to the remote host use the TNSEND command and the identifier of the connection (usually the host name). For example if the host, *mercury*, prompts you for your login ID on starting a connection, you would enter:

```
TNSEND mercury user01
```

To reduce the amount of typing required, you can set up your own equate. For example, you might want to assign the period (**.**) as an equate to send data to the host, *mercury*. To do this, enter the following OCS command:

```
EQ . -START $TNCALL COMMAND=TNSEND ID=mercury DATA=
```

The above equate means that to send data (for example, the login ID requested in the earlier example), you need only enter:

```
.user01
```

Note: The TNSEND command is itself an equate which is set up as follows:

```
EQUATE TNSEND+ -START $TNCALL COMMAND=TNSEND ID=
```

Automating Commands Issued to Remote Hosts

You can use an NCL procedure to automate the starting of a connection and the issuing of commands to the remote host to which the connection has been made. For example, you might want to create a procedure that logs on to Router1 and checks its interfaces. The following example shows how you can do this.

```
.
.
.
-* Start the connection
-*
&INTCMD TELNET Router1 MODE=LINE
.
.
.
-*
-* Receive messages from the router
-*
&INTREAD SET
.
.
.
-*
-* Send the SHOW INTERFACES command to the router
-*
&INTCMD TNSEND Router1 SHOW INTERFACES
```

You could then process the results of the SHOW INTERFACES command and reformat the display for an operator or you could send a monitor message if an error situation is detected.

Note: Issuing &INTCLEAR TYPE=ALL causes the connection to be terminated. Use &INTCLEAR TYPE=ANY to clear any queued messages and continue processing.

For details about Management Services commands, see the *NCL User's Guide* and the *Management Services Command Reference* manual.

Ending a Telnet Connection in Line Mode or OCS Take-over Mode

Depending on the type of host to which you are connected, it is likely that you will be disconnected when you issue the logoff command appropriate to that host. If this is not the case, use the TNDISC command (or, in OCS takeover mode, the F3 (Disconnect)) to end the connection.

Sending Control Codes or Special Characters to the Remote Host

It is likely that you will occasionally need to send control codes such as Ctrl-C, or special characters such as [to the remote host; for example, Ctrl-D to log off from the host.

The control character is used to do this and it is specified when you start a Telnet connection, either in the Control field of the Options window (see the section "Issuing Telnet Commands"), or in the CTRL operand of the TELNET command (described in the *Management Services Command Reference*). The default control character is ¢, but you can change this by using the CTRL operand of the TELNET command.

The control character has two distinct purposes:

- To simulate the Ctrl key; for example, ¢C becomes Ctrl-C.
- To send characters that are otherwise not supported on 3270 keyboards:

To send...	Enter...
[	¢{
]	¢}
Del (X'7F')	¢#
NUL (X'00')	¢0
Esc (X'1B')	¢2
X'1C'-X'1F'	¢3-¢6

Using the ---more--- Prompt

You can send a string of text without the usual ENTER character (CRLF or CR) by ending the string with ¢ and the ENTER key. For example, you might want to send a single space in response to a --more-- prompt. To do this, press the space bar, type ¢ and press ENTER.

Note: Cisco routers support the command: TERMINAL LENGTH 0, which prevents them from using the --more-- prompt.

Chapter 22

Diagnosing Resources by Using SNMP

This chapter contains the following topics:

- What Is SNMP?
- Accessing the SNMP Functions
- Browsing and Changing the Value of MIB-II Objects
- Testing Connectivity
- Tracing a Route
- Listing Managed Resources

What Is SNMP?

SNMP is an application protocol that is able to manage a multi-vendor TCP/IP environment by enabling:

- The retrieval and updating of objects in Management Information Bases (MIBs) such as MIB-II, the standard SNMP MIB
- The issuing of *traps* to report unexpected events

By using the SNMP functions of NetMaster for TCP/IP you can use a TCP/IP communication link to various SNMP managers—to send commands to them, and to receive SNMP responses.

The SNMP Standard Management Information Base (MIB)

MIB-II is a fundamental part of SNMP that contains object definitions describing the resources within a TCP/IP internet. These objects are organized in logical groups and each object is uniquely identified by an Abstract Syntax Notation One (ASN.1) identifier (a sequence of digits) that is constant and platform-independent. The SNMP *get* and *set* commands enable you to browse and, if you have write authority, change the value of MIB-II objects that have write access. The value of a particular object is known as a *variable*.

Accessing the SNMP Functions

If you need to access management information about TCP/IP hosts by means of SNMP, use the SNMP functions.

The SNMP functions work with the following SNMP managers:

- IBM TCP/IP—directly
- TCPaccess—directly
- NetView for AIX—by using a REXEC connection
- HP OpenView—by using a REXEC connection

To access the SNMP functions, enter **/IPDIAG.SF** at the ===> prompt. The SNMP : Function Menu is displayed. The name of the manager last entered in the SNMP Manager Name field is retained, as is its description.

```
PROD------------------------- SNMP : Function Menu --------------------$SP003
Select Option ===>

   M   - Access MIB-II                                          SNMP
   P   - Ping a Device                                          -
   T   - Trace a Network Route                                  -
   R   - List Managed Resources (OpenView and NetView only)     -
   A   - Manager Administration List                            -
   X   - Exit

SNMP Manager Name .........+ MVSTCP__              ( Required R Optional M P T)
             Description ... MVS TCP/IP

Device Name ................ ____________________________________________________
                             ____________________________________________________
       IP Address .......... ________________
```

SNMP : Function Menu Options

The tasks that you can perform from this menu are shown in the following table, which also indicates where you can find a detailed description of these tasks:

To perform the task ...	Use option ...	Described in the section...
Accessing the MIB-II Access Menu to browse and change the value of MIB-II objects	**M**	"Browsing and Changing the Value of MIB-II Objects"
Sending a ping to check whether a device is accessible through the network	**P**	"Testing Connectivity"
Tracing a route through an internet to determine the exact route taken by a packet.	**T**	"Tracing a Route"
Listing the TCP/IP resources managed by a specific SNMP network management station	**R**	"Listing Managed Resources"
Browsing and updating the Manager Maintenance List	**A**	The *Unicenter NetMaster Network Management for TCP/IP Administrator Guide*

Input Fields on the SNMP : Function Menu

The fields on the SNMP : Function Menu are as follows:

SNMP Manager Name—The user-assigned name for the remote or native SNMP manager. If you type a question mark (?) in this field, a list of existing managers is displayed and you can select the one you require.
(Optional, and *Prompted. Mandatory* for the R option*)*

Listing SNMP Managers

```
PROD------------------------ CAS : Valid Value List --------------------------4
Select Option ===>                                              Scroll ===> CSR

          Field: MANAGER NAME

          Full Value   Description
   1    - MANAGER1     at Head Office, IS Department
   2    - MANAGER2     at Head Office, Accounts Department
   3    - MANAGER3     at Head Office, Marketing Department
   4    - MANAGER4     at Head Office, Sales Department
          **END**
```

Description—The text string associated with the particular instance of the SNMP manager (in the NetMaster for TCP/IP configuration file). Displayed when the SNMP Manager Name field is completed.
(Derived, Protected)

Device Name—The user-assigned name of a target TCP/IP device under the control of the remote or native SNMP manager. If you have selected the List Managed Resources option, enter the full name of the device. Complete this field *or* the IP Address field, but not both.
(Optional)

IP Address—The IP address of a target TCP/IP device under the control of the remote or native SNMP manager. Complete this field *or* the Device Name field, but not both.
(Optional)

If you enter a value in either the Device Name or the IP Address field, then select option **M**, **P**, or **T**, the value entered is redisplayed in the corresponding field on subsequent panels.

Note: If you want the device IP address (rather than the device name) to be used to locate a device, you must ensure that the Device Name field is blank.

Browsing and Changing the Value of MIB-II Objects

SNMP acts on MIB-II objects or variables, which are individual data items that are clustered in logical groups. NetMaster for TCP/IP enables you to browse (or get) a group of SNMP objects, and to change (or set) the value of individual objects, if you have write authority. Get is the default action.

Accessing MIB-II

To gain access to MIB-II, you do the following:

1. On the SNMP : Function Menu panel, enter the name or the IP address of the device for which the MIB is being accessed.

   Note: If you want the IP address to be used to identify the target device, the Device Name field must be blank.

2. Choose the **M** - Access MIB-II option. The SNMP MIB-II Access Menu is displayed. The Device Name or (Device) IP Address field contains the value entered on the SNMP : Function Menu panel.

```
PROD---------------------- SNMP : MIB-II Access Menu ------------------$SP010
Select Option ===>

   S   - System Group
   I   - Interfaces Group
   A   - Address Translation Group
   IP  - IP Subgroups
   IC  - ICMP Group
   T   - TCP Subgroups
   U   - UDP Subgroups
   E   - EGP Subgroups
   SN  - SNMP Group
   GS  - Get/Set/MIB-II Walk
   X   - Exit

Device Name ................ ________________________________________________
                             ________________________________________________
       IP Address .......... _______________
Community Name ............. ________________________________________________


 F1=Help      F2=Split     F3=Exit      F4=Return
                           F9=Swap
```

SNMP : MIB-II Access Menu Options

The tasks that you can perform from this menu are shown in the following table, which also indicates where you can find a detailed description of these tasks:

To perform the task ...	Use option ...	Described in the sections...
Browse and change the values of system group objects for a specified device	**S**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Browse and change the values of interfaces group objects for a specified device	**I**	"Browsing and Changing MIB-II Objects by Doing a MIB Walk"
Browse and change the values of address translation group objects for a specified device	**A**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Browse and change the values of IP objects for a specified device within a subgroup	**IP**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Browse Internet Control Message Protocol (ICMP) group objects for a specified device	**IC**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Browse and change the values of Transmission Control Protocol (TCP) objects for a specified device within a subgroup	**T**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Browse User Datagram Protocol (UDP) objects for a specified device within a subgroup	**U**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Browse and change the values of Exterior Gateway Protocol (EGP) objects for a specified device within a subgroup	**E**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Browse and change the values of Simple Network Management Protocol (SNMP) group objects for a specified device	**SN**	"Browsing MIB-II Group Objects" and "Changing the Value of MIB-II Objects"
Get or set a series of MIB-II objects one after the other	**GS**	"Browsing and Changing MIB-II Objects by Doing a MIB Walk"

Browsing MIB-II Group Objects

To get or display MIB-II group objects from the MIB-II Access Menu, you do the following:

1. At the Select Option ==> prompt, enter the mnemonic for the option that you require.
2. If you did not complete either the Device Name or IP Address field when selecting the Access MIB-II option from the SNMP : Function Menu, enter one of these values in the appropriate field.
3. If a community name other than the supplied default (public) is required by your organization, enter the community name that is associated with the device name.

   The community name, which is a security feature, is validated during the get operation. If the retrieval attempt fails due to an invalid community name, an error message is displayed.
4. Press ENTER to get the specified MIB-II group or to display the menu listing the various subgroups that make up the group.
5. If a menu is displayed (as is the case for the Subgroups options on the MIB-II Access Menu), select the required menu option to view a particular subgroup.

   See the following figure for the subgroups menus.

```
PROD--------------------- SNMP : MIB-II IP Group Menu -------------------$SP104
Select Option ===>

   I   - IP Group
   A   - IP Address Table
   R   - IP Routing Table
   AT  - IP Address Translation Table
   X   - Exit
-------------------------------------------------------------------------------
PROD--------------------- SNMP : MIB-II TCP Group Menu ------------------$SP106
Select Option ===>

   T   - TCP Group
   C   - TCP Connection Table
   X   - Exit
-------------------------------------------------------------------------------
PROD--------------------- SNMP : MIB-II UDP Group Menu ------------------$SP107
Select Option ===>

   U   - UDP Group
   L   - UDP Listener Table
   X   - Exit
-------------------------------------------------------------------------------
PROD--------------------- SNMP : MIB-II EGP Group Menu ------------------$SP108
Select Option ===>

   E   - EGP Group
   N   - EGP Neighbour Table
   X   - Exit
```

The initial (or single, if there is only one) panel of group objects, such as the System Group panel (see the following figure) is displayed in Get mode. The device name or (device) IP address (or both) that you entered on a previous panel is redisplayed.

To move to the next group of MIB-II data for the specified device, enter the GETNEXT command. To move forward to the next panel or backward to the previous panel in a sequence, use the FORWARD or BACKWARD command.

For example, if you issue the GETNEXT command from the System Group panel, the first Interfaces Group panel for the device is displayed. You can then use the FORWARD command to go to the second Interfaces Group panel for the device.

```
PROD--------------------- SNMP: MIB-II System Group -----------------NETSYSGRP1
Command ===>

 Device Name ................ pluto
        IP Address .......... 123.168.9.57

 Description ...... 80486 DOS 6.0
                    Windows 3.10 Enhanced Mode
                    NetManage SNMP 3.11

 Object ID ........ .iso.org.dod.internet.private.enterprises.567

 Up Time .......... 3 days, 23:15:39 (342939280 msecs)
 Contact .......... Jim Jones
-------------------------------------------------------------------------------
Name ............. pluto.dept.company.com

Location ......... North Silicity branch office, Arcadia

Services ......... Internet,End-to-end,Application
```

Changing the Value of MIB-II Objects

If there are objects on the panel you are browsing that have write access, the SET function key (F4) is displayed at the bottom of the panel.

If, for example, you have write authority and you want to change the value of one or more of the objects on the SNMP MIB-II System Group panel, proceed as follows:

1. From the SNMP MIB-II System Group panel in Get mode, use the SET command (or function key) to change to Set mode.

   The display is modified to show which fields have write access, and to include a Community Name input field, as shown below.

Changing the Value of MIB-II System Group Objects

```
PROD---------------------- SNMP: MIB-II System Group ---------------NETSYSGRP1
Command ===>

Device Name ................ pluto
       IP Address .......... 192.168.9.57
Community Name (for SET command) ...

Description ...... 80486 DOS 6.0
                   Windows 3.10 Enhanced Mode
                   NetManage SNMP 3.11

Object ID ........ .iso.org.dod.internet.private.enterprises.567

Up Time .......... 3 days, 23:15:39 (342939280 msecs)
Contact  .......... Jim Jones_____________________________________________________
--------------------------------------------------------------------------------
Name .............coriander_____________________________________________________

Location ........ North Silicity branch office, Arcadia_____________________
                  ____________________________________________________________
Services ......... Internet,End-to-end,Application
```

2. If the community name that is required to change the value of objects is different to the one that is required to browse objects, enter the appropriate community name.
3. Overwrite existing data in the field or fields that you want to alter, with new data. In the case of *enumerated fields* (which are displayed as a character string, followed by an integer in parentheses), you enter one of the following:
   - The entire value—character string plus integer in parentheses
   - Just the integer, followed by a blank (no parentheses)
   - Just the character string, followed by a blank

   For example, you can enter one of the following valid value strings in the Desired State field on the MIB-II Interfaces panel:
   - Up (1)
   - Down (2)
   - Testing (3)
4. Use the ACTION command (or function key) to initiate the set action—one of the following messages is displayed to indicate whether the set succeeded or failed:

   ```
   Set successful or Set failed
   ```

If an error occurs, the full text of the error message is displayed, along with the name of each object for which the set failed.

Browsing and Changing MIB Objects by Doing a MIB Walk

A MIB walk is an SNMP function that enables you to examine MIB-II objects sequentially.

During a MIB walk you can also browse or change the value of an individual object. The procedure is as follows:

1. On the SNMP MIB-II Access Menu panel, enter the name or IP address of a device and choose the **GS** - Get / Set / MIB-II Walk option.

   The SNMP MIB-II Object Get / Set panel is displayed, in Get mode. The Device Name or IP Address field contains the value entered on the SNMP : Function Menu panel (or the SNMP MIB-II Access Menu). The Object Descriptor, ID, and Value fields contain the name, identifier, and current value of the first System Group object. (This is because the System Group is the first MIB-II group.)

Getting a MIB-II Object via a MIB Walk

```
PROD---------------------- SNMP: MIB-II Object Get/Set -----------------------
Command ===>

Device Name ................ pluto

       IP Address ..........

Object Descriptor .......... System.Syscontact.0_____________________________

       ID ................... .1.3.6.1.2.1.1.4.0_____________________________
                                ________________________________________________
       Value ..... Jim Jones

F1=Help      F2=Split      F3=Exit      F4=Set                      F6=Getnext
                           F9=Swap
```

2. Enter either the descriptor or the identifier of the object that precedes the one you want to get. (If you choose to enter an object identifier, you must delete the default object descriptor first.)
3. Use the GETNEXT command (or function key) to display the required object value, in Get mode.
4. If you want to change the object value, see the section “Changing the Value of MIB-II Objects” for the procedure.
5. If you want to get or set further object values, and you are in Set mode, use the CANCEL command (or function key) to return to Get mode.
6. Enter a new object name or identifier, or use the GETNEXT command (or function key) to move to the next sequential object.

Fields on the SNMP : MIB-II Object Get/Set Panel

The fields on the SNMP : MIB-II Object Get / Set panel are as follows:

Object Descriptor—A unique string that identifies the object. You must complete either this field or the (object) Identifier field, when in Get mode, to display the current value of the object. This field is protected in Set mode.

ID—The unique ASN.1 identifier of the object. You must complete either this field or the Object Name field, when in Get mode, to display the current value of the object. This field is protected in Set mode.

Value—The current value of this object for the specified device. This field is protected in Get mode, but can be overwritten in Set mode, if the object has write access.

Note: There are a limited number of MIB-II objects that have write access. The presence of the F4=Set key at the bottom of the MIB-II Object Get / Set panel indicates that the value of that object can be altered.

The SNMP MIB-II walk panel is displayed, in Set mode. It includes a Community Name field, which you must complete if the community name (password) for updating a MIB-II object value differs from the community name for browsing a MIB-II object value.

Setting a MIB-II Object via a MIB Walk

```
PROD----------------------- SNMP: MIB-II Object Get/Set -----------------------
Command ===>

Device Name ................ pluto

       IP Address ..........
Community Name (for SET command) ...

Object Descriptor .......... System.Syscontact.0

       ID ................... .1.3.6.1.2.1.1.4.0

       Value ..... Jim Jones_____________________________________________________

F1=Help      F2=Split      F3=Exit                                    F6=Action
                           F9=Swap                                   F12=Cancel
```

Testing Connectivity

The PING command is used primarily to test whether a device is reachable through the network or not. The PING command can also be used to do the following:

- Determine the IP address of a device
- Determine the network transit time for packets of varying sizes
- Determine whether all packets sent (if you requested more than one ping) reached their destination

Initiating a Ping

If you want to ping a device, the procedure is as follows:

1. On the SNMP : Function Menu panel, enter the name or the IP address of the device you want to access.

   Note: If you want the IP address to be used to identify the target device, the Device Name field must be blank.

2. Select the **P** - Ping a Device option.

   The SNMP : Ping TCP/IP Device panel is displayed. The Device Name or (Device) IP Address field contains the value or values entered on the SNMP : Function Menu panel.

```
PROD----------------------- SNMP: Ping TCP/IP Device --------------NETSYSGRP1
Command ===>

Device Name ................ pluto_____________________________________________

       IP Address .......... _______________
Packet Size ................ 64__        Number of Times to Ping .... 1_
Detailed Output (Yes/No) ... NO_

   (Either Device Name or Device IP Address must be specified)
```

3. Complete any of the other fields on this panel, as required.
4. Use the ACTION command to begin the ping procedure.

The definitions for the fields on the SNMP : Ping a TCP/IP Device panel are as follows:

Device Name—The user-assigned name of a target TCP/IP device under the control of the remote or native SNMP manager. If you have selected the List Managed Resources option, enter the full name of the device. Complete this field *or* the IP Address field, but not both. This field is mandatory on this panel if the IP Address field is not completed.

IP Address—The IP address of a target TCP/IP device under the control of the remote or native SNMP manager. Complete this field *or* the Device Name field, but not both. This field is mandatory on this panel if the Device Name field is not completed.

Packet Size—The number of bytes to be sent; minimum 40, maximum 65519. (This value defaults to 64.)
(Optional)

Number of Times to Ping—The number of times to send the PING command, ranging from 1 to 50. (Defaults to 5).
(Optional)

Detailed Output—YES indicates that you require detailed output about each ping attempt; NO indicates that you only require summary information. (Defaults to NO.)
(Optional)

Note: The effect of requesting detailed output varies from one SNMP manager to another. In some cases, it makes little practical difference whether you specify YES or NO

Interpreting Responses to a Ping

See the following figure for the possible responses to the PING command. If you did not supply the device IP address initially, it is returned by a successful ping.

```
PROD---------------------- SNMP: Ping TCP/IP Device ----------------NETSYSGRP1
Command ===>                                                 Scroll ===> PAGE

Device Name ............... pluto.dept.company.com_____________________
                            ____________________________________________
       IP Address ......... 123.168.9.57___
Packet Size ............... 64__        Number of Times to Ping .... 10
Detailed Output (Yes/No) ... YES

------------------------------ Ping Statistics -------------------------------
 Packets transmitted ........ 10        Round trip (ms) minimum .... 6
         received ........... 10                        average .... 67
         lost (%) ........... 0                         maximum .... 143

  ICMP Seq    IP Address          Bytes       Time
  Number                          Received    (msec)
   0          123.168.9.57        64          242
   1          123.168.9.57        64           11
   2          123.168.9.57        64           82
   3          123.168.9.57        64           97
   4          123.168.9.57        64          168
   5          123.168.9.57        64           38
   6          123.168.9.57        64           31
   7          123.168.9.57        64            6
   8          123.168.9.57        64           18
   9          123.168.9.57        64          128
 **END**
```

When a Ping Is Successful

If you specify detailed output and your request is successful, the results are displayed below the input fields on the SNMP : Ping TCP/IP Device panel.

Each ping generates a response, and these responses can flow on to additional panels. If you specify NO detailed output, or if the ping is unsuccessful, only the ping statistics are displayed. (The exact format of this information might vary slightly, according to the response received.)

The output column headers displayed on the SNMP : Ping a TCP/IP Device panel below the input fields are as follows:

ICMP Seq No—The sequential number of a packet sent by the PING command; for example, 3 (the fourth packet sent). If one or more numbers in the sequence are missing, this indicates that some packets sent by ping are failing to reach their destination.

IP Address—The IP address of the device.

Bytes Received—The number of bytes in the packet received by the destination device (which should be the same as the packet size).

Time (msec)—The time taken to perform the ping (round trip), in milliseconds.

The information listed under the heading Ping Statistics (displayed even if NO is specified in the Detailed Output field) is as follows:

- The number of packets transmitted and received
- The percentage of packets lost during the ping procedure
- The minimum, average, and maximum times taken to perform a round trip, in milliseconds

When a Ping Is Unsuccessful

If a ping is unsuccessful (for example, if the target device is not responding), the statistics displayed indicate that all packets were lost, (see the following figure). If you enter an invalid target device name, or if a request times out before a response is received, an appropriate error message is displayed on the third line of the screen.

```
PROD---------------------- SNMP: Ping TCP/IP Device ----------------NETSYSGRP1
Command ===>                                                 Scroll ===> PAGE

Device Name ................ venus

       IP Address ..........
Packet Size ................ 64          Number of Times to Ping .... 1
Detailed Output (Yes/No) ... YES

------------------------------ Ping Statistics -------------------------------
 Packets transmitted ........ 1        Round trip (ms) minimum ....
         received ........... 0                        average ....
         lost (%) ........... 100                      maximum ....
```

Tracing a Route

It is possible to obtain a hop-by-hop record of the route taken by a packet through an internet, starting from the source device and finishing at the destination device.

Selecting a Trace Method

You can use one of the following commands to trace a TCP/IP route:

- The SNMP FINDROUTE command (not for an IBM TCP/IP manager)
- The ICMP TRACEROUTE command (the default used)

The differences between traceroute and findroute are as follows:

Traceroute	Findroute
Displays round trip times	Does not display round trip times
Is dependent on the Internet Control Message Protocol (ICMP), many implementations of which are known to be unreliable	Is dependent on SNMP, requiring all gateways along the path it is tracing to support SNMP
Can be used by all supported managers	Cannot be used by IBM TCP/IP

Initiating a Trace

To initiate a trace, you use the following procedure:

1. On the SNMP : Function Menu panel, enter the name or the IP address of the destination device.

   Note: If you want the IP address to be used to identify the target device, the Device Name field must be blank.

2. Select the **T** - Trace a Network Route option. The SNMP : Trace TCP/IP Route panel is displayed. The Destination Device Name or (destination device) IP Address field contains the value or values entered on the SNMP : Function Menu panel.

```
PROD---------------------- SNMP: Trace TCP/IP Route ----------------NETSYSGRP1
Command ===>

Target Device Name ......... saturn_____________________________________________
                             _____________________________________________________
              IP Address ... 123.168.6.45___
Trace method (ICMP=Traceroute/SNMP=Findroute) .... ICMP

(For ICMP trace)
Packet size ................ 40__       Max Time to Live (Hops) .... 30


   (Either Device Name or Device IP Address must be specified)
```

3. Complete the Trace Method field, to indicate whether you are requesting an SNMP Findroute or an ICMP Traceroute.
4. If you specify ICMP, you can change the default values in the remaining fields.
5. Use the ACTION command to begin the Findroute or the Traceroute action.

The definitions for the fields on the SNMP : Trace a TCP/IP Route panel are as follows:

Target Device Name—The name of the target TCP/IP host. This field is mandatory on this panel if the IP Address field is not completed.

IP Address—The IP address of the target TCP/IP host. This field is mandatory on this panel if the Target Device Name field is not completed.

Trace Method—The method to be used to perform the trace—ICMP, if the Traceroute method is to be used, or SNMP, if the Findroute method is to be used. (This value defaults to ICMP.)

If you specify SNMP in the Trace Method field, the Packet Size and Max Time to Live fields are ignored. If you specify ICMP, you can use the default values, or enter alternative values.

Packet Size—The number of bytes to be sent to the target host by the Traceroute action. You might, for example, want to check whether both large and small packets are reaching their destination. (This value defaults to 40; range is 40 to 65519).

Max Time to Live (Hops)—The maximum number of hops to be traced along a route, ranging from 2 to 255. (This value defaults to 30.)

The results of a Traceroute or a Findroute procedure are displayed below the input fields on the SNMP : Trace TCP/IP Route panel.

```
PROD---------------------- SNMP: Trace TCP/IP Route ----------------NETSYSGRP1
Command ===>                                                 Scroll ===> PAGE

Target Device Name ......... saturn.dept.company.com_____________________________
                                                                                
              IP Address ... 123.168.6.45___
Trace method (ICMP=Traceroute/SNMP=Findroute) .... ICMP

(For ICMP trace)
Packet size ................ 40__       Max Time to Live (Hops) .... 30

  Hop  Resource Name                          Resource IP          Round Trip Time
  No.                                          Address                (msec)
   1   saturn                                192.168.6.45        32   14   91
 **END**
```

The definitions of the column headers for both Findroute and Traceroute results are as follows:

Hop No.—The sequential number of the hop along the route you are tracing; for example, 3 (the third hop in the trace sequence).

Resource Name—The name of the resource associated with the device representing the hop.

Resource IP Address—The IP address of the resource associated with the device representing the hop.

Round Trip Time—The time taken for a packet to reach the resource associated with the hop and return to the source, in milliseconds (not provided by Findroute).

```
PROD----------------------- SNMP: Trace TCP/IP Route ---------------NETSYSGRP1
Command ===>                                                 Scroll ===> PAGE

Target Device Name ......... saturn.dept.company.com_____________________________
                                                                                
              IP Address ... 123.168.6.45___
Trace method (ICMP=Traceroute/SNMP=Findroute) .... SNMP

(For ICMP trace)
Packet size ................ 40__       Max Time to Live (Hops) .... 30

 Source              Source Address   Next Hop             Next Hop Address
 hubble.dept.company  123.168.1.1     saturn.dept.company.  123.168.6.45
 **END**
```

If a trace is unsuccessful, the results are as follows:

- If you used the Traceroute method, either an error message is displayed on line three of the screen, or asterisks are displayed in the Round Trip Time columns for unsuccessful hops.
- If you used the Findroute method, details of successful hops are displayed, and an error message identifies the hop encountered that does not support SNMP.

Listing Managed Resources

Each SNMP manager can control a number of TCP/IP resources, which NetMaster for TCP/IP allows you to list. This function is not supported by native managers (such as IBM TCP/IP).

Note: NetMaster for TCP/IP lists, like the NetView for AIX and HP OpenView icon maps, are built using information stored in the topology database. This does not always reflect the up-to-the-minute state of resources, as it is only updated periodically.

When you want to list members of a particular class of resource managed by SNMP, you do the following:

1. Select the **R** - List Managed Resources option from the SNMP : Function Menu to display the SNMP : List Managed Resources Menu.

```
PROD------------------- SNMP : List Managed Resources Menu -------------$SP011
Select Option ===>


   N   - Networks
   D   - Devices on a Network
   I   - Interfaces on a Device
   A   - All
   X   - Exit

Network IP Address .... _______________
Device Name ........... ____________________________________________________
```

2. Select the class of resource that you want to display, or select the **A** - All option to list all managed resources.

   If the function you select is not supported, the following error message is displayed:

   `OPTION IS NOT SUPPORTED FOR MANAGER TYPE` *xxxx*

If the function is supported, the appropriate list of managed resources is displayed. The actions given on line four of the panel indicate which actions can be applied to listed entries. One or more of the following actions may be listed, but only one can be applied at a time:

- **M**—access MIB-II data for a device
- **P**—test if a device is reachable by using the PING command
- **T**—trace the route taken by a packet sent to a device
- **L**—list devices or list interfaces (where appropriate)

3. If you want to apply one of the available actions to a listed item, enter the mnemonic for the action beside that item.

The column headers on the managed resource lists are as follows:

Device Local Name—The name of the device on the local network, such as *frodo.*

Type—The type of managed network device.

IP Address—The IP address of the device.

Link Level Address—The media-dependent physical address, such as an Ethernet or a token-ring address.

Status—See the following table for the valid values for NetView for AIX and HP OpenView.

If the status is ...	The resource is ...
Acknowledged	not being monitored. This status is set by the user for an object whose status is unimportant.
Down	not functioning.
Marginal	functioning but defective. This status is set by an application.
Unknown	of a status that cannot be determined. This status is set by an application.
Unmanaged	not being monitored. This status is set by the user for an object whose status is unimportant.
Up	functioning.
UserStatus 1	of a status defined by an administrator. See the *AIX SystemView NetView for AIX User's Guide* for more information.
UserStatus 2	of a status defined by an administrator. See the *AIX SystemView NetView for AIX User's Guide* for more information.

Listing Managed Resources

See the following figure for the left-hand panel and part of the right-hand panel of the Managed Routers list for a NetView for AIX manager.

```
PROD------------------------ SNMP: Managed Routers --------------------------
Command ===> right                                          Scroll ===> CSR

                                        S/M=MIB-II Access P=Ping T=Traceroute

    Device Local Name              IP Address       Status
    venus                          123.168.8.127    Up
    saturn                         123.168.6.45     Up
    saturn                         123.168.6.45     Up
-------------------------------------------------------------------------------
    Device Local Name              Link Lvl Address
    venus                          0x000030407215
    saturn                         0x000030180075
    saturn                         0x0000301800F5
```

See the following figure for a sample list of Managed Networks.

```
PROD------------------------ SNMP: Managed Networks -------------------------
Command ===>                                                Scroll ===> CSR

                                                    S/L=List devices P=Ping

    IP Address       Status
    123.168.1.0      Up
    123.168.2.0      Up
    123.168.3.0      Up
    123.168.4.0      Up
    123.168.5.0      Up
    123.168.6.0      Up
    123.168.7.0      Marginal
    **END**
```

See the following figure for the left-hand panel and part of the right-hand panel of the Managed Network Devices list. The Type column displays information only if the type is known by the connected OpenView or NetView system.

```
PROD---------------------- SNMP: Managed Network Devices ----------------------
Command ===> right                                          Scroll ===> CSR

                      L=List Interfaces S/M=MIB-II access P=Ping T=Traceroute

    Device Local Name              IP Address       Status
    venus                          123.168.8.127    Up
    saturn                         123.168.6.45     Up
    pluto                          123.168.9.57     Up
    jupiter                        123.168.4.15     Up
    **END**
-------------------------------------------------------------------------------
                       L=List Interfaces S/M=MIB-II access P=Ping T=Traceroute

    Device Local Name              Type                        Link Lvl Address
    venus                                                      0x000030407215
    saturn                                                     0x0000301800F5
    pluto                                                      0x10005A3A4451
    jupiter                                                    0x00008370BB1F
    **END**
```

Note: NetMaster for TCP/IP lists, like the NetView for AIX and HP OpenView icon maps, are built using information stored in the topology database. This does not always reflect the up-to-the-minute status of resources, as it is only updated periodically.

Listing SNMP-managed Device Interfaces

```
 PROD-------------------- SNMP: Managed Device Interfaces ---------------------
Command ===>                                                  Scroll ===> CSR

                                        S/M=MIB-II access P=Ping T=Traceroute

    IP Address       Status          Link Level Address
    123.168.1.1      Up              0x000030180075
    123.168.2.1      Up              0x0000301800F5
    123.168.3.1      Up              0x000030180035
    123.168.4.1      Up              0x000000000C17
    123.168.5.1      Up              0x0000301800B5
    **END**
```

See the following figure for the left-hand and right-hand panels of the Managed Resources list.

```
PROD----------------------- SNMP: Managed Resources --------------------------
Command ===> right                                            Scroll ===> CSR

                                        S/M=MIB-II access P=Ping T=Traceroute

    Device Local Name               IP address       Status
    mercury                         123.168.2.66     Up
    mars                            123.168.3.81     Down
    venus                           123.168.8.127    Up
    uranus                          123.168.7.23     Down
    **END**
-------------------------------------------------------------------------------
                                        S/M=MIB-II access P=Ping T=Traceroute

    Device Local Name               Type                      Link Lvl Address
    mercury                                                   0xAA0004009437
    mars                                                      0xAA0003050473
    venus                                                     0x000030407215
    uranus                                                    0x00608C66C420
    **END**
```

Glossary

Abstract Syntax Notation—See ASN.1.

ASN.1 (Abstract Syntax Notation One)—An OSI data description language, used by SNMP to define objects in Management Information Bases (MIBs). ASN.1 defines a number of data types and these are used in specifying objects.

Agent—See Network Management Agent.

BER (Basic Encoding Rules)—An OSI standard for encoding ASN.1 data structures, used by SNMP for encoding its messages.

Bridge—A communications device that connects two or more LANs and passes traffic between them.

Bus and Tag Channel—IBM channel, developed in the 1960s, incorporating copper multiwire technology. Replaced by the ESCON channel. See also *ESCON Channel* and *Parallel Channel*.

Channel Card—Channel attachment interface for Cisco routers. The channel card is used to connect a host mainframe to a router to provide functions such as SNA and TCP/IP connectivity and offloading of TN3270 processing. An example of a channel card is the Channel Interface Processor (CIP).

CIP (Cisco Channel Interface Processor)—See *Channel Card.*

CMCC (Cisco Mainframe Channel Connection)—Also known as channel card. See *Channel Card.*

CNM (Communications Network Management)—IBM term for its SNA management facilities.

Community—An administrative definition of a set of SNMP agents and managers (management stations), used to grant common access rights.

Community Name—A password used by SNMP network management stations to access remote network management agents.

CS (Communications Server for OS/390)—IBM's TCP/IP stack released with OS/390 version 2.5. It combines IBM SNA/APPN and TCP/IP expertise to manage heterogeneous networking environments in a consolidated manner.

CSM (Communications Storage Manager)—IBM's buffer management technology. CSM enables authorized host application programs to put data in buffers that can be addressed and accessed by other authorized host application programs without any need to copy the data.

Datagram—The message unit transmitted by the Internet Protocol layer. It can be regarded as the TCP/IP counterpart of the Basic Information Unit in SNA networks.

Echo—A special ICMP signal sent to another node, which generates a reply. This is done as a test of connectivity.

Enterprise Extender (EE)—A data link control (DLC) that supports High-Performance Routing (HPR) connections over Internet Protocol (IP) networks. To the HPR network, the IP backbone appears to be a logical link. The SNA traffic is carried over the IP network in User Datagram Protocol (UDP) datagrams.

ESCON (Enterprise System Connection)—IBM channel architecture that specifies a pair of fiber-optic cables, with either LEDs or lasers as transmitters, and a signaling rate of 200 Mbps. See also *LED*.

ESCON Channel —IBM channel for attaching mainframes to peripherals such as storage devices, backup units, and network interfaces. This channel incorporates fiber channel technology. The ESCON channel replaces the bus and tag channel. Compare with *Parallel Channel*. See also *Bus and Tag Channel*.

Fragment—A subunit of a datagram. Datagrams that are too large for a particular subnetwork to transport are split into fragments. These fragments are recombined by the IP layer at the destination node.

Gateway—A device that connects two or more networks with different network architectures and routes traffic between them. A gateway also acts as a protocol translator. (The term *router* is more commonly used.)

Host—A network node that also performs application processing, and has an associated Internet address.

IBM TCP/IP—Any IBM TCP/IP stack.

ICMP (Internet Control Message Protocol)—A protocol defined within the Internet Protocol (IP) for the purpose of performing various control functions, including: detecting and reporting network problems, testing connectivity, and tracing network routes.

INMC (Inter-Management Services Connection)—This facility allows SOLVE systems running in a network to communicate with each other, providing general-purpose data transfer within the network.

Internet—A collection of linked networks running TCP/IP and related protocols. By convention, this word, when used with a capital I, denotes the (one) worldwide internetwork that has evolved from the ARPANET. The word *internet* with a lower case *i* denotes any particular implementation that uses the same protocol suite.

Internet Address—The logical address assigned to a node's interface to a network, for use by the Internet Protocol (IP). This address is a 32-bit number that is conventionally written as a sequence of the four decimal values of the bytes, starting from the highest value and separated by dots (periods); for example, 149.124.176.6.

Internet Protocol (IP)—The protocol that routes packets across multiple subnetworks (such as LANs and WANs). It is analogous to the protocol for the network layer in the OSI Reference Model.

Internet Suite of Protocols—The set of protocols in common usage on the Internet. These include IP, TCP, ICMP, SNMP, SMTP, Telnet, and FTP.

ISO—The International Organization for Standardization.

LAN—Local Area Network.

LED—Light emitting diode; a semiconductor device that emits light produced by converting electrical energy. Status lights on hardware devices are typically LEDs.

Management Information Base (MIB)—A definition of a set of data items used for management purposes. The items are known as objects, and represent features of network resources that can be managed. See also *MIB-II*.

MIB-II—The standard set of object definitions that all SNMP agents are required to support.

MIB Walk—The process of proceeding sequentially through a MIB, to examine object values. The sequence of objects is defined by the MIB hierarchy.

Multicast—Sent to more than one destination. Usually refers to a network message.

OS/390—An IBM operating system.

NCL (Network Control Language)—The interpretive language of the Management Services. This language allows logical procedures (programs) to be developed externally and executed by the Management Services, on command. NCL contains a wide range of logic, built-in functions, and arithmetic facilities that can be used to provide powerful monitoring and automatic control functions.

NCL Procedure—A member of the Management Services procedures dataset, which comprises NCL statements and SOLVE or VTAM commands. The NCL statements and other commands are executed using an &CALL statement (or an EXEC or START command) that specifies the name of the procedure.

Neighbor—A logically adjacent node. This concept is used in routing protocols such as EGP.

Network Error Warning System—See NEWS.

NEWS (Network Error Warning System) —A feature of NetMaster that is used to provide network error and traffic statistics and error alert messages.

Network Management Agent—A management program that executes at a managed network node, for the purpose of managing resources at that node under the direction of one or more network managers. The agent responds to SNMP commands from the network management station and sends SNMP traps to the station.

Network Manager—A management program that executes at a network node, for the purpose of allowing a network operator to send management commands to remote nodes and to receive event reports from these remote nodes. The network manager sends SNMP commands to network management agents at nodes, requesting the agents to act on Management Information Base (MIB) objects. It receives SNMP responses and traps from the agents, the latter indicating significant events at the nodes.

NMVT (Network Management Vector Transport)—A type of SNA request/response Record Unit (RU), used for transmitting management commands and data through an SNA network.

Node—A connection point in a communications network.

NTS (Network Tracking System)—A feature of NetMaster, NTS is an integrated network management and problem determination system that operates in multi-domain networks. It accumulates traffic statistics on a session and resource basis to allow network performance monitoring.

Object—An item of managed data maintained within a Management Information Base. Individual instances (values) of objects are also referred to as MIB variables.

Object Identifier—An ASN.1 data type. An object identifier is a sequence of integers separated by dots (periods). Each integer represents a level in a registration tree. The sequence of integers is used to uniquely identify an object in a Management Information Base. For example, the object identifier 1.3.6.1.2.1.1.1.0 identifies the sysDescr object in MIB-II.

Octet—An eight-bit value, synonymous with the term *byte*.

OCS (Operator Console Services)—A Management Services feature that provides general operational control and an advanced operator interface to VTAM for network management.

OSA (Open Systems Adapter)—An IBM hardware device for OS/390 that acts as a combination of a communications controller and a channel.

OSI (Open Systems Interconnection)—A set of ISO standards for communication between computer systems.

Open Systems Interconnection—See OSI.

Parallel Channel—Channel that uses bus and tag cables as a transmission medium. Compare with *ESCON Channel*. See also *Bus and Tag Channel*.

Ping—A program that enables a test message to be sent to another node, requesting a reply, for the purpose of testing connectivity. This program uses ICMP Echo messages. Formally defined as Packet InterNet Grope, hence the acronym.

Protocol—A set of rules for achieving communication across a network.

RFC 768—An Internet standard (Request For Comment) that defines UDP packets.

RFC 791—An Internet standard (Request For Comment) that defines IP packets.

RFC 792—An Internet standard (Request For Comment) that defines ICMP packets.

RFC 793—An Internet standard (Request For Comment) that defines TCP packets.

RFC 1213—An Internet standard (Request For Comment) that defines MIB-II.

Router—A network node that receives packets, examines their destination addresses and makes decisions about the communication paths on which to forward them. Today, most routers support multiple network protocols, so the term router is replacing the term *gateway*, which was previously used to denote protocol translation and packet routing.

Server—A computer or a process that responds to a request for service from one or more clients.

Simple Network Management Protocol—See SNMP.

SNA (Systems Network Architecture)—This term describes the logical structure, formats, protocols, and operational sequences for transmitting communications data through the communication system in an IBM network. Intended by IBM as a set of standards that allows the integration of all the different IBM hardware/software products into a universal network. Introduced in 1974.

SNMP (Simple Network Management Protocol)—A protocol for management of internetworks, originally designed for management of devices running TCP/IP. The term is also commonly used for the architecture on which this protocol is based.

SNMP Manager—A management system that uses the Simple Network Management Protocol. Also known within SNMP as a network management station.

Subnet Mask—A 32-bit number used to partition the IP address space of an internetwork, to allow traffic to be routed to multiple subnetworks.

TCP (Transmission Control Protocol)—A transport level protocol that runs on top of IP and provides guaranteed delivery in sequence of data across an internetwork.

TCP/IP (Transmission Control Protocol/Internet Protocol)—Commonly used to signify the Internet protocol suite.

Transmission Control Protocol/Internet Protocol—See TCP/IP.

Trap—An SNMP event report.

UAMS (Userid Access Maintenance Subsystem)—The security component of Management Services that supports the definition of authorized users and their associated function and privilege levels.

UDP (User Datagram Protocol)—A transport level protocol that allows multiplexing of IP datagrams between different application processes but does not guarantee delivery. It is used by SNMP.

Unicast—Sent to a single destination. Usually refers to a network message.

Variable—See *Object*.

VTAM (Virtual Telecommunications Access Method)—A suite of programs that controls communication between terminals and application programs.

WAN—Wide Area Network.

Z/OS—An IBM operating system.

Index

$

$LOG command, 6-16

2

2216 routers
- channel information, 10-6
- information, 10-4
- performance, 10-7
- TN3270 LUs, 10-6
- TN3270 PUs, 10-5
- TN3270 server information, 10-5

A

action lists, 2-8

actions
- CICS Socket Connection List, 3-11
- Connection List, 3-13
- Telnet Connection List, 3-9

actions, specific
- Connection List, 20-16
- Delete, 17-8
- Drop, 4-9
- History, 8-6
- Information, 17-3
- Insert, 17-8
- Interfaces, 7
- Lookup, 4-9, 7
- MIB-II, 7
- Packet List, 20-16
- Ping, 7
- Repeat, 17-8
- Routing Table, 7
- Select, 17-3
- Session List, 4-8
- System Information, 7
- Telnet, 7
- VTAM Display, 4-7

active traces, 20-7

activity log
- connection activity, 4-13
- FTP activity, 4-12
- Obeyfile processing, 6-16
- Telnet activity, 4-11

address space performance, 13-3

Alert Monitor, 2

alerts
- commands, 3, 6
- details, 5
- history, 6
- log, 6
- monitoring, 2
- printing details, 6
- responding to, 4
- trouble tickets, 4

analyzing
- network data, 17-10
- SNA sessions, 4-8

ASN.1 object identifiers, 22-2

B

bar charts, 18-5

C

canceling changes to a record, 2-11

channel card
- performance, 9-20
- TCP Offload information, 9-17
- TN3270 server log, 9-10, 9-12

channel card information, 9-7
- application, 9-7
- channel, 9-8
- CLAW, 9-13
- CLAW subchannels, 9-14
- internal LAN, 9-19
- internal LAN adapters, 9-19
- SNA (CSNA), 9-18
- TN3270 server, 9-9

channel information, 2216 router, 10-6

Channel Interface Processor (CIP), 9-2

Channel Port Adapter (CPA), 9-2

CICS
- command server interface, 14-6
- resources
  - information, 14-4
  - performance, 14-9
- server, starting, 14-7
- socket connections, 3-9, 3-16
- Socket Management, connections, 14-4
- transaction, starting, 14-8

Cisco channel card, 9-2

Cisco Mainframe Channel Connection (CMCC). *See* channel card

CLAW
- information, 9-13
- subchannels, 9-14

commands
- alert history, 6

commands, alert monitor, 3

commands, IP resource monitor, 5-3
- for class ASMON, 13-2
- for class CICMON, 14-3
- for class CIP, 9-5
- for class CSM, 12-2
- for class EE, 11-3
- for class OSA, 8-3
- for class ROUTER, 10-2
- for class STACK (IBM), 6-2
- for class STACK (TCPaccess), 7-2

commands, line
- NSLOOKUP, 4-9
- PING, 4-4
- TRACEROUTE, 4-6

commands, specific
- $LOG, 6-16
- CTRACE, 20-5
- DATE, 6
- FILTER, 5-3, 8
- FINDROUTE, 22-15
- GET, 22-5
- GETNEXT, 22-8, 22-10
- LOCATE, 2-10, 20-15
- LOCATE, 3-6, 20-17
- NETSTAT, 3-18
- NSLOOKUP, 4-9
- PING, 4-2, 4-4, 22-12
- PRINT, 20-26
- PROFILE, 5-3
- SET, 22-5, 22-8
- SORT, 3-6, 9-16, 20-14, 20-17
- SPLIT, 2-15
- SWAP, 2-15
- TELNET, 21-12
- TRACEROUTE, 4-6, 22-15

commands, Telnet, 21-10

Communications Storage Manager. *See* CSM

community names, validation, 22-7

configuration
- changing
  - by using an Obeyfile, 6-15, 6-16
  - by using the Edit key, 7-11
- client, 6-12, 6-13
- datasets, 6-10
- FTP, 6-13, 6-14
- TCP/IP, 6-10

Connection List action, 20-16

connection lists, 3-2
- actions
  - CICS Socket, 3-11
  - general, 3-13
  - Telnet, 3-9
- CICS Socket, 3-10
- criteria
  - CICS Socket, 3-9
  - general, 3-12
  - Telnet, 3-7

general, 3-12
Telnet, 3-8

connections
activity log, 4-13
diagnosing, 4-10
dropping, 4-9
listing
criteria, 3-7
general, 3-11
multiple systems, 3-5
locating information, 3-6
searching, 17-4
Socket Management, 14-4
sorting lists, 3-6
specific, 3-18
Telnet, 21-2
Telnet, searching, 17-5
testing, 4-2
to remote host, 21-12
workload performance, 4-18

connectivity
problem diagnosis, 3-2, 3-14
testing, 3-2, 3-14, 22-12

console commands, 6-9, 7-9

control codes, Telnet, 21-16

CSM
performance, 12-5
usage, 12-4

CSNA information, 9-18

CTRACE
saving trace data, 20-10
starting, 20-5
stopping, 20-9

D

data entry panels, 2-10

data transfer problems, diagnosis, 3-2

data validation, 2-11

datasets
FTP.DATA, 6-13
Obeyfile, 6-15
PARMS, 7-11
PROFILE.TCPERROR, 6-14
PROFILE.TCPIP, 6-10

Delete action, 17-8

devices
dropping a connection, 4-9
links, 6-4, 6-5, 7-4
looking up a device name, 4-9
on a network, 22-18
OSA, 8-5
configuration, 8-5
performance, 8-6
tracing a route, 4-4

diagnosing
connections, 4-10
data and protocol problems, 4-10
performance and connectivity, 3-2, 3-14
resource attributes, 18-4
Telnet problems
connection, 9-3
response time, 4-13
throughput, 4-15

Domain Name Server, 6-19

Drop action, 4-9

dropping a connection, 4-9

E

entering data, 2-11

Enterprise Extender
overview, 11-2
performance, 11-7
sessions list, 11-5
summarized information, 11-4
UDP port activity, 11-6
XCA Major Nodes, 11-4

enumerated fields, 22-9

error log, TCP/IP, 6-14

errors, packet tracing, 20-26

ESCON connection hierarchy, 10-6

events
performing custom search, 17-6
searching database, 17-4
searching file transfer events, 17-5

extracting data to a file, 17-10

F

fields
- enumerated, 22-9
- mandatory, 2-11
- optional, 2-11
- prompted, 2-11

file transfer events, searching, 17-5

filing data, 2-11

FILTER command, 5-3, 8

Find function, 2-10

FINDROUTE command, 22-15
- results, 22-17

FS Telnet, starting connections, 21-4

FTP
- activity in the log, 4-12
- configuration (FTP.DATA), 6-13
- monitoring workload performance, 4-17

FTP.DATA, 6-13, 6-14

function keys, Telnet-specific, 21-5

G

get failure message, 22-7

Get mode, 22-8, 22-10

GETNEXT command, 22-10

graphical representation of a host, 3-15

H

header data
- ICMP, 20-25
- IP, 20-25
- TCP, 20-24
- UDP, 20-24

help, online, 2-13

History Report List, 17-9

horizontal scrolling, 2-9

HP OpenView remote manager, 22-2

I

ICMP traceroute support, 22-15

Index Menu, 2-12

Information action, 17-3

Initialization in Progress panel, 2-2

Insert action, 17-8

interface workload performance, 6-9, 7-9

Interfaces action, 7

interfaces on a device, 22-18

internal LAN
- adapters, 9-19
- channel card information, 9-19

interpreting responses
- to a ping, 4-3
- to a traceroute, 4-5

IP address, finding, 3-19

IP node monitor, 7
- adding nodes, 8
- filtering, 8
- monitor group, 8

IP resource classes, 5-4
- ASMON, 13-2
- CICMON, 14-2
- CIP, 9-4
- CSM, 12-2
- EE, 11-2
- OSA, 8-3
- ROUTER, 10-2
- STACK
  - IBM, 6-2
  - TCPaccess, 7-2

IP resource monitor, 5-2, 6-2, 7-2, 8-2, 9-4, 10-2, 11-2, 12-2, 13-2, 14-2
- adding an IP resource, 5-4
- commands, 5-3
  - for class ASMON, 13-2
  - for class CICMON, 14-3
  - for class CIP, 9-5
  - for class CSM, 12-2
  - for class EE, 11-3
  - for class OSA, 8-3
  - for class ROUTER, 10-2
  - for class STACK (IBM), 6-2
  - for class STACK (TCPaccess), 7-2

customizing, 5-3
defaults, 5-3
filtering, 5-3

issuing console commands, 6-9, 7-9

K

knowledge base definitions
customizing panel access, 2-13

L

line commands
NSLOOKUP, 4-9
PING, 4-4
TRACEROUTE, 4-6

list types, 2-8

lists, specific
2216 TN3270 LU List, 10-6
2216 TN3270 PU List, 10-5
2216 TN3270 Server Information, 10-5
Active Packet Trace List, 20-7
CICS Socket Connection List, 3-10
Connection List, 3-12
Enterprise Extender Session List, 11-6
Managed Device Interfaces, 22-21
Manager Name valid value list, 22-4
OSA Device List, 8-5
Ping Result List, 4-3
Session List, 11-5
TCPaccess Parameters Library List, 7-10
Telnet Connection List, 3-8
Trace Route Result List, 4-5

LOCATE command, 2-10, 3-6, 20-15, 20-17

locating records, 2-10

log
activity, 4-10
TN3270 server, 4-10, 9-12

logging off, 2-3

logging on, 2-2

Lookup action, 4-9, 7

LUs
finding name, 3-18
for a PU, 9-11

M

mandatory fields, 2-11

masks, 3-18

menus, specific
Connections, 3-2
MIB-II Access, 22-5
MIB-II Group, 22-7
Network Diagnosis Functions, 2
Packet Trace, 20-2
Packet Tracing, 20-2
SNMP Function, 22-3
SNMP Function Menu, 8

messages
help, 2-14
invalid community name (get failure), 22-7
session awareness, 4-15
set acknowledgement, 22-9
set failure error, 22-9
TPA, 4-14

MIB
definition, 22-2
walk, 22-10

MIB-II, 22-2, 22-5, 22-7, 22-10
group objects, 22-7
object values, 22-10

MIB-II action, 7

mini trace, Cisco Telnet LU, 9-4

mode
Get, 22-8, 22-10
Set, 22-8

monitor group, IP nodes, 8

monitoring
active alerts, 2
channel cards, 9-3
IP nodes, 7

monitors
IP resources, 5-2, 6-2, 8-2, 9-4, 10-2, 11-2, 12-2, 13-2, 14-2

multiple select lists, 2-8

multisystem support, listing connections, 3-5

N

navigation
- splitting screens, 2-15
- swapping screens, 2-15
- toggling between windows, 2-15
- working in two windows, 2-15

NetMaster for TCP/IP
- features and benefits, 1-2
- logging on, 2-2
- SNMP functions, 22-2

NETSTAT command, 3-18

NetView for AIX remote manager, 22-2

networks
- analyzing data, 17-10
- managed networks, 22-18

NSLOOKUP command, 4-9

numbered lists, 2-8

O

Obeyfile
- changing the configuration, 6-15, 6-16
- creating a new dataset member, 6-17
- editing
  - dataset, 6-16
  - dataset member, 6-17
- viewing contents and results, 6-16

online help, 2-13
- messages, 2-14

Open Systems Adapters. *See* OSA
- device list, 8-5
- performance, 8-4
- utilization, 8-4

optional fields, 2-11

OSA, 8-2
- configuration, 8-6

P

Packet List action, 20-16

Packet Trace Menu, 20-2

packet tracing, 20-4
- active traces, 20-7
- connections within a trace, 20-16
- CTRACE
  - starting, 20-5
  - stopping, 20-9
- data for a selected packet, 20-19
- errors, 20-26
- formatted packets, 20-21
- header data
  - ICMP, 20-25
  - IP, 20-25
  - TCP, 20-24
  - UDP, 20-24
- IP header fields, 20-22
- IP options, 20-22
- packet details, 20-22
- packets in a trace, 20-18
- printing formatted packet details, 20-26
- protocol data, 20-24
  - ICMP, 20-25
  - IP, 20-25
  - TCP, 20-24
  - UDP, 20-24
- protocol header fields, 20-23
  - ICMP, 20-23
  - TCP, 20-23
  - UDP, 20-23
- saved traces, 20-11, 20-12
- saving trace data, 20-10
- starting a trace, 20-6
- stopping a trace, 20-7
- TCP options, 20-23

panels
- customizing access, 2-13
- data entry, 2-10

panels, specific
- 2216 Router Channel Information, 10-6
- 2216 Router Information, 10-4
- 2216 TN3270 LU List, 10-6
- 2216 TN3270 PU List, 10-5
- 2216 TN3270 Server Information, 10-5
- Active Packet Trace List, 20-7
- Alert Display, 5
- Alert Monitor, 2
- Browse FTP.DATA Dataset, 6-13

Browse Print Queue, 16-3
Browse Profile Dataset, 6-11
Browse PROFILE.TCPERROR Dataset, 6-14
Browse TCPaccess PARMS Dataset, 7-11
Browse TCPIP.DATA Dataset, 6-12
CICS Socket Connection List, 3-10
CICS Socket Connection List Criteria, 3-10
CICS Socket Connections Display, 3-16
Cisco Channel Card Information, 9-7
Cisco Channel Information, 9-8
Cisco CLAW Information, 9-13
Cisco CLAW Subchannel List by Card, 9-15
Cisco CLAW Subchannel List by Host, 9-16
Cisco CLAW TN3270 LU List, 9-11
Cisco CLAW TN3270 PU List, 9-10
Cisco CLAW TN3270 Server Information, 9-9
Cisco CSNA Information, 9-18
Cisco Internal LAN Adapters, 9-19
Cisco Internal LAN Information, 9-19
Cisco TCP Offload Information, 9-17
Cisco Telnet LU Mini Trace, 9-4
Confirm Stop, 20-8
Connection Information (TCPaccess), 3-14
Connection List, 3-12
Connection List Criteria, 3-12
Connections Display, 3-17
Connections Menu, 3-2
CSM Usage by Buffer, 12-4
CSM Usage by Job, 12-4
Device Links, 6-5, 7-4
Device Links List, 6-4, 7-4
Edit PROFILE Dataset, 6-11
Enterprise Extender Session List, 11-6
Formatted Packet Display
    Format A, 20-19
    Format B, 20-20
    Format C, 20-21
History Report List, 17-3
Initialization In Progress, 2-2
Interface List, 5
IP Node Monitor, 7
IP Node Monitor Details, 8
IP Resource Monitor, 5-2, 6-2, 7-2, 8-2, 9-4, 10-2, 11-2, 12-2, 13-2, 14-2
Line Printer (LPD) Diagnostics, 16-2, 16-4
Managed Device Interfaces List, 22-21
Manager List, 22-4
MIB-II Object Get/Set
    Get mode, 22-10
    Set mode, 22-11
Monitor 2216 Router Performance, 10-7
Monitor Address Space Performance, 13-3, 18-3
Monitor Channel Card Performance, 9-20
Monitor CICS Performance, 14-9
Monitor CSM Performance, 12-5
Monitor Enterprise Extender Performance, 11-7
Monitor Open Systems Adapter Performance, 8-4
Monitor Stack IP Performance History, 6-7, 7-7
Node Display - LINE, 11-5
Node Display - XCA MAJN, 11-4
Obeyfile Confirm, 6-15
Obeyfile PDS List, 6-15
Open Systems Adapter Summary, 8-4
OSA Configuration, 8-7
OSA Device List, 8-5
Packet Details on the Formatted Packet Display, 20-22
Packet List (Part 1), 20-18
Packet Trace IP Address List, 20-14
Packet Trace IP Connection List, 20-16
Ping Result List, 4-3
Ping TCP/IP Device, 22-12
Problem Telnet LUs, 6-18
Profile Configuration Datasets, 6-11
Resource Detail Graph, 18-4, 18-6
Resource Summary Graph, 18-4, 18-6
Routing Table, 6
Save Trace Data, 20-10
Save Trace Warnings/Errors, 20-10
Saved Trace List, 20-12
Session List, 11-5
SocketMgmt Bounce Confirmation
    SB command, 14-5
    SSB command, 14-6
SocketMgmt Connections List, 14-4
SocketMgmt Information, 14-4
SocketMgmt Server StartConfirmation, 14-7
SocketMgmt Transaction StartConfirmation, 14-8
Stack IP Performance Metrics, 6-8, 7-8
Start CTRACE, 20-5
Stop CTRACE, 20-9
System Group
    Get mode, 22-8
    Set mode, 22-9
System Information, 4
TCP/IP Stack Workload Status, 6-19
TCPaccess Parameters Library List, 7-10
Telnet, 21-3
Telnet Cluster List, 6-20
Telnet Connection List, 9-3
Telnet Connection List Criteria, 3-3, 3-7
Telnet Connections Display, 3-15
Telnet Server Status, 6-20
TN3270 Server Log, 9-12
Trace Route Result List, 4-5
Transaction Path Analysis, 4-15

UDP Port Activity, 11-6
User Password Change, 2-4
XCA Major Node Summary, 11-4

parameters library, 7-10

PARMS dataset
browsing, 7-11
changing, 7-12
creating a new member, 7-12

password, changing, 2-3

performance
2216 routers, 10-7
address space, 13-3
channel card, 9-20
CICS resource, 14-9
connection workload, 4-18
CSM, 12-5
Enterprise Extender, 11-7
FTP workload, 4-17
history, 18-2
interface workload, 6-9, 7-9
IP stack
history, 6-7, 7-7
metrics, 6-8, 7-8
monitor, 18-4
Open Systems Adapters, 8-4
problem diagnosis, 3-2, 3-14
real-time reports, 18-2
resource attributes, 18-4
sampling, 17-9
searching data, 17-9
stack interface workload, 6-9, 7-9
Telnet workload, 4-19

performing
a ping, 4-2
a traceroute, 4-4

Ping action, 7

PING command, 4-2, 4-4, 22-12
interpreting responses, 4-3
possible responses, 22-13
statistics returned, 22-14

Ping Result List, 4-3

PRINT command, 20-26

printers
deleting print queue entry, 16-3
managing problems, 16-2
querying status, 16-2
sending test print, 16-4

printing
formatted packet details, 20-26
reports, 17-11

privilege levels (user access authority), 2-5

problems
diagnosis, 3-2
SNA, 4-7

PROFILE command, 5-3

PROFILE.TCPERROR, 6-14

PROFILE.TCPIP, 6-11

prompted fields, 2-11

protocol data, 20-24
ICMP, 20-25
IP, 20-25
TCP, 20-24
UDP, 20-24

protocol header fields, 20-23

PUs for a server, 9-10

R

real-time performance reports, 18-2

records, canceling changes, 2-11

Repeat action, 17-8

reports
actions, 17-3
checking print queue, 17-12
defining to Netmaster for TCP/IP, 17-12
listing, 17-3
offline archival system, 17-13
overview, 17-2
printing, 17-11
viewing, 17-3

resource classes, IP, 5-4

Resource Detail Graph, 18-4

Resource Summary Graph, 18-4

resources
diagnosing attributes, 18-4
SNMP managed resources, 22-18
TCP/IP, status, 3-18

response time
diagnosing problems, 4-13
Telnet, 4-13

routers, managed, 22-18

routing table, 6, 7

Routing Table action, 7

S

saving
data, 2-11
packet trace data, 20-10

scrolling, 2-8

search, custom, 17-6

searching
connections, 17-4
events database, 17-4
file transfer events, 17-4
performance data, 17-9
Telnet connections, 17-5
Telnet display data, 21-7

security, 2-5

Select action, 17-3

selecting panels
all panels, 2-12
by Index Menu, 2-12
by Panel Display List, 2-12
by sequence number, 2-12

Session List action, 4-8

sessions list, Enterprise Extender, 11-5

SET command, 22-8
failure message, 22-9

Set mode, 22-8

single select lists, 2-8

SNA
analyzing sessions, 4-8
checking VTAM status of an LU, 4-7
problems, 4-7

SNMP
definition, 22-2
functions, 8, 22-2
managed resources, 22-18
Manager List, 22-4
managers, 22-2
standard MIB, 22-2

SNMP Function Menu, 8, 22-3

Socket Management
CICS resource performance, 14-9
connections, 14-4
shutting down and restarting, 14-5
starting a CICS server, 14-7
starting a CICS transaction, 14-8
stopping and restarting command server interface, 14-6

SORT command, 3-6, 9-16, 20-14, 20-17

special characters, Telnet, 21-16

SPLIT command, 2-15

splitting screens, 2-15

stack IP performance
history, 6-7, 7-7
metrics, 6-8, 7-8

status of resources, 3-18

SWAP command, 2-15

swapping screens, 2-15

System Group
browsing details, 22-8
changing the value of objects, 22-8
sample screen in Get mode, 22-8
sample screen in Set mode, 22-9
write access, 22-8

system information, 4

System Information action, 7

T

TCP Offload information, 9-17

TCP options, 20-23

TCP/IP
commands, 22-2
configuration (PROFILE.TCPIP), 6-10
error log, 6-14
stack workload, 6-19
tracing routes, 4-4

TCP/IP local manager, 22-2

TCPIP.DATA, 6-12, 6-13

Telnet
activity on the user log, 4-11
commands, 21-10
connecting to remote hosts, 21-2
connection details, 21-11
Connection List, 3-8, 9-3
connections
displaying, 3-15
SNA problems, 4-7
Connections Display, 3-15
control codes, 21-16
displaying connections from a foreign host, 3-15
editing display text, 21-5
ending connection, 21-11
function keys, 21-6
LUs, 6-18
printing from display, 21-8
response times, 4-13
searching display data, 21-7
server workload, 6-19
setting options, 21-9
SNA-related problems, 4-7
special characters, 21-16
starting connections, 9-10, 21-3, 21-4
to router, 9-8
workload performance, 4-19

Telnet action, 7

testing connectivity, 3-2, 3-14, 4-2

throughput, diagnosing, 4-15

tip of the day, 2-13

TN3270 server
information, 9-9, 10-5
LUs, 10-6
PUs, 10-5

TN3270 server log, 9-12

toggling between windows, 2-15

Trace Route Result List, 4-5

TRACEROUTE
command, 22-15
interpreting responses, 4-5
results, 22-17
line command, 4-6

tracing
a TCP/IP route
using the FINDROUTE command, 22-15
using the TRACEROUTE command, 22-15
an SNMP route, 22-15
IP packets in TCP/IP, 20-2

Transaction Path Analyzer, 4-13, 4-15, 4-16

trouble tickets for an alert, 4

U

UAMS security features, 2-5

UDP port activity, Enterprise Extender, 11-6

UPDATE mode, switching to, 2-10

User Password Change panel, 2-4

utilization, Open Systems Adapters, 8-4

V

validating
community name, 22-7
data, 2-11

vertical scrolling, 2-9

VTAM Display action, 4-7

VTAM status, 4-7

W

working in two windows, 2-15

workload
connections, 4-18
FTP, 4-17
multiple TCP/IP stacks, 6-19
stack interface, 6-9, 7-9
Telnet, 4-19
Telnet servers, 6-19

Workload Manager (WLM), 6-19

X

XCA major nodes, Enterprise Extender, 11-2
summarized information, 11-4